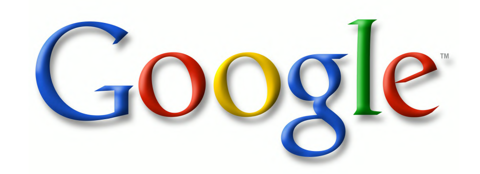






Journal

für die

reine und angewandte Mathematik.

In zwanglosen Heften.

Herausgegeben

von

A. L. Crelle.

Mit thätiger Beförderung hoher Königlich-Preufsischer Behörden.

Sieben und zwanzigster Band.

In vier Heften.

Mit vier lithographirten und einer gedruckten Tafel.

Berlin, 1844.
Bei G. Reimer.
Et se trouve à Paris chez Mr. Bachelier (successeur de Mme Ve Courcier).
Libraire pour les Mathématiques etc. Quai des Augustins No. 55.

Inhaltsverzeichnifs
des sieben und zwanzigsten Bandes, nach den Gegenständen.

Reine Mathematik.

1. Analysis.

Nr. der Abhandlung.		Heft.	Seite.
1.	Über die Bildung der Endgleichung, welche durch Elimination einer Variabeln aus zwei algebraischen Gleichungen hervorgeht, und die Bestimmung ihres Grades. Von Herrn Dr. *Otto Hesse* zu Königsberg in Pr.	I.	1
2.	Encyklopädische und elementare Darstellung der Theorie der Zahlen. Vom Herausgeber dieses Journals.	I.	6
10.	Fortsetzung davon.	II.	107
26.	Weitere Fortsetzung davon.	IV.	330
3.	Théorèmes sur les formes cubiques, et solution d'une équation du quatrième degré à quatre indéterminées. Par Mr. *G. Eisenstein* à Berlin.	I.	75
4.	Über die Anzahl der quadratischen Formen, welche in der Theorie der complexen Zahlen zu einer reellen Determinante gehören. Von Herrn *G. Eisenstein*, Stud. zu Berlin.	I.	80
5.	Allgemeine Auflösung der Gleichungen von den ersten vier Graden. Von Herrn Stud. *G. Eisenstein* zu Berlin.	I.	81
8.	Untersuchungen über die cubischen Formen mit zwei Variabeln. Von Herrn Stud. *G. Eisenstein* zu Berlin.	II.	89
9.	Über eine merkwürdige identische Gleichung. Von Herrn Stud. *G. Eisenstein* zu Berlin.	II.	105
11.	Zusätze zu der Abhandlung über die Methode der kleinsten Quadrate, No. 22. im 26. Bande d. Journ. Von Herrn Dr. *Reuschle*, Prof. am Gymnasium zu Stuttgart.	II.	182
12.	Bemerkungen zu den elliptischen und Abelschen Transcendenten. Von Herrn Stud. *G. Eisenstein* zu Berlin.	II.	185
13.	Note extraite d'une lettre adressée à l'éditeur par Mr. *E. Catalan*, Répétiteur à l'école polytechnique de Paris.	II.	192
14.	Transformations remarquables de quelques séries. Par Mr. *G. Eisenstein* à Berlin.	III.	193
16.	Theoria novi multiplicatoris systemati aequationum differentialium vulgarium applicandi. Auctore *C. G. J. Jacobi*, prof. ord. math. Regiomonti.	III.	199
17.	Beiträge zur Kreistheilung. Von Herrn Stud. *G. Eisenstein* zu Berlin.	III.	269
18.	Notiz über einige Producten-Ausdrücke. Von Hrn. Dr. *Stern* in Göttingen. (Auszug aus einem Briefe desselben an den Herausgeber dieses Journals.)	III.	279
20.	Elementare Ableitung einer merkwürdigen Relation zwischen zwei unendlichen Producten. Von Hrn. Stud. *G. Eisenstein* zu Berlin.	IV.	285

Nr. der Abhandlung.		Heft.	Seite.
21.	Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Von Herrn Stud. G. *Eisenstein* zu Berlin.	IV.	289
22.	Über die Anzahl der quadratischen Formen in den verschiedenen complexen Theorieen. Von Herrn Stud G. *Eisenstein* zu Berlin.	IV.	311
23.	Einfacher Algorithmus zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$. Von Herrn Stud. G. *Eisenstein*.	IV.	317
24.	Eigenschaften und Beziehungen der Ausdrücke, welche bei der Auflösung der allgemeinen cubischen Gleichungen erscheinen. Von Herrn Stud. G. *Eisenstein* zu Berlin.	IV.	319
25.	Neuer und elementarer Beweis des Legendreschen Reciprocitäts-Gesetzes. Von Herrn Stud. G. *Eisenstein* zu Berlin.	IV.	322
27.	Erwiderung auf den Artikel 23. im 26sten Bande dieses Journals. Von Herrn Prof. *Minding* in Dorpat.	IV.	379

2. Geometrie.

6.	Resultate der Auflösung von drei geometrischen Aufgaben; für Liebhaber des algebraischen Calculs. Von Herrn Prof. Dr. *Lehmus* zu Berlin.	I.	84
15.	Der Kreis-Umfang für den Durchmesser 1 auf 200 Decimalstellen berechnet von Herrn Z. *Dahse* in Wien.	III.	198
17.	Beiträge zur Kreistheilung. Von Herrn Stud. G. *Eisenstein* zu Berlin.	III.	269

Aufgaben und Lehrsätze.

7.	Von Herrn Stud. G. *Eisenstein* zu Berlin.	I.	86
19.	Von Verschiedenen.	III.	281
Druckfehler.		II. 192.	III. 284.
	Fac-simile einer Handschrift von *Kepler*.	I.	
	- - - - - - *Lexell*.	II.	
	- - - - - - *Fourier*.	III.	
	- - - - - - *Carnot*.	IV.	

Druckfehler im 26ten Bande.

Seite 162 Zeile 6 v. u. st. linea l. lineas
— — — 5 v. u. st. ductae l. ductas
— 169 — 7 v. o. nach „ergo aequatio coni" ist einzuschalten: „quum $b-a$, $b-c$ oppositis gaudeant signis"
— 173 — 15 v. o. st. $\frac{bs}{bt}=\frac{A^2}{B^2}$ lies $\frac{bs}{bt}=\frac{B^2}{A^2}$
— 175 — 13 v. o. sind die Worte hinter „folgende Construction" bis Z. 14. „angewendet werden kann," wegzulassen.

Druckfehler im 27ten Bande.

Seite 282 Zeile 17 v. o. statt $-\frac{1}{4}(p-q)^2$ lies $-\frac{1}{4}(p-q)^2$
— 285 — 3 v. o. st. ungleichen l. unendlichen

1.

Über die Bildung der Endgleichung, welche durch Elimination einer Variabeln aus zwei algebraischen Gleichungen hervorgeht, und die Bestimmung ihres Grades.

(Von Herrn Dr. *Otto Hesse* zu Königsberg in Pr.)

Die Aufgabe, eine Variable aus zwei algebraischen Gleichungen zu eliminiren, kann auf die Bildung einer aus den Coëfficienten der nach den Potenzen der Variabeln geordneten Gleichungen zusammengesetzten Determinante zurückgeführt werden, und die Eigenschaften der Endgleichung ergeben sich leicht aus der Untersuchung dieser Determinante. Die Determinanten sind aber ein Gegenstand vielfältiger Untersuchungen gewesen, so dafs es kaum mehr als der Zurückführung der ersten Aufgabe auf die zweite bedarf, um den Grad der Endgleichung zu bestimmen, oder damit verwandte Aufgaben zu lösen. Die Idee, die Endgleichung unter der Form einer gleich 0 gesetzten Determinante zu betrachten, finden wir zuerst vom Herrn Professor *Jacobi* Bd. 15. S. 101 dieses Journ. ausgeführt. Während aber an dem angeführten Orte die Componenten der Determinante bestimmte Functionen der Coëfficienten der nach den Potenzen der Variabeln geordneten Gleichungen sind, werden wir im Folgenden die Endgleichung unmittelbar aus den erwähnten Coëfficienten zusammensetzen, wodurch wir eine bequeme Einsicht in die Natur dieser Gleichung erhalten.

Die gegebenen und nach den Potenzen der Variable x geordneten Gleichungen vom $n$ten und $m$ten Grade seien:

$$A_0 = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0 x^0 = 0,$$
$$B_0 = b_m x^m + b_{m-1} x^{m-1} + b_{m-2} x^{m-2} + \dots + b_1 x + b_0 x^0 = 0.$$

Setzt man alsdann $x^p A_0 = A_p$, $x^q B_0 = B_q$, so erhält man, wenn man der Gröfse p nach einander die Werthe $m-1$, $m-2$, ... 1, 0, und der Gröfse q die Werthe $n-1$, $n-2$, ... 1, 0 zutheilt:

$$\begin{aligned} A_{m-1} &= a_n x^{m+n-1} + a_{n-1} x^{m+n-2} + a_{n-2} x^{m+n-3} + \dots a_1 x^m + a_0 x^{m-1}, \\ A_{m-2} &= \qquad + a_n x^{m+n-2} + a_{n-1} x^{m+n-3} + \dots a_2 x^m + a_1 x^{m-1} + a_0 x^{m-2}, \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ A_0 &= \qquad\qquad a_n x^n + \dots + a_1 x + a_0 x^0, \end{aligned}$$

$$
\begin{aligned}
B_{n-1} &= b_m x^{m+n-1} + b_{m-1} x^{m+n-2} + b_{m-2} x^{m+n-3} + \dots\, b_1 x^n + b_0 x^{n-1}, \\
B_{n-2} &= \qquad\qquad b_m x^{m+n-2} + b_{m-1} x^{m+n-3} + \dots\, b_2 x^n + b_1 x^{n-1} + b_0 x^{n-2}, \\
&\cdot\;\cdot \\
B_0 &= \qquad\qquad\qquad\qquad\qquad a_m x^{n-1} + \dots + b_1 x + b_0 x^0.
\end{aligned}
$$

Betrachtet man in diesen Gleichungen die verschiedenen Potenzen von x, nämlich x^{m+n-1}, x^{m+n-2}, ... x, x^0, als die Unbekannten, so erhält man durch Auflösung dieser, wie zu bemerken, lineären Gleichungen, Brüche von demselben Nenner, der mit P bezeichnet werden mag. Dieser Nenner ist die Determinante der Coëfficienten der Unbekannten. Setzt man nun $A_0 = A_1 \dots = A_{m-1} = B_0 = B_1 \dots = B_{n-1} = 0$, so hat man $m+n$ lineäre und homogene Gleichungen in Rücksicht auf die $m+n$ Unbekannten. Diese Gleichungen können im Allgemeinen nicht zugleich erfüllt werden. Die Bedingung, unter welcher dieses möglich ist, oder, mit andern Worten, das Resultat der Elimination ist bekanntlich: $P = 0$.

Diese Gleichung ist die gesuchte Endgleichung. Denn wenn man x den Werth der Variabeln bedeuten läfst, welcher den beiden Gleichungen $A_0 = 0$ und $B_0 = 0$ zu gleicher Zeit genügt, so hat man $A_0 = A_1 = \dots = A_{m-1} = B_0 = B_1 = \dots = B_{n-1} = 0$. Eliminirt man daher aus obigen $m+n$ Gleichungen, in welchen $A_0 = A_1 = \dots = A_{n-1} = B_0 = B_1 = \dots = B_{n-1} = 0$ gesetzt worden, sämmtliche Potenzen von x, als ob sie verschiedene Unbekannten wären, so wird das Resultat der Elimination die genannte Gleichung $P = 0$ sein, welche mit $A_0 = 0$ und $B_0 = 0$ zugleich erfüllt wird und nicht mehr die Variable x enthält.

Um die einzelnen Glieder der Determinante P zu bilden, kann man sich bequem folgender Tafel bedienen.

	1	2	3	....	....	....	....	....	....	....	$m+n-1$	$m+n$
1	a_n	a_{n-1}	a_{n-2}	....	a_2	a_1	a_0	0	0	0	0	0
2	0	a_n	a_{n-1}	....	a_3	a_2	a_1	a_0	0	0	0	0
3	0	0	a_n	....	a_4	a_3	a_2	a_1	a_0	0	0	0
⋮												
$m-1$	0	0	0	0	a_n	a_{n-1}	a_{n-2}	...	a_2	a_1	a_0	0
m	0	0	0	0	0	a_n	a_{n-1}	....	a_3	a_2	a_1	a_0
$m+1$	b_m	b_{m-1}	b_{m-2}	....	b_2	b_1	b_0	0	0	0	0	0
$m+2$	0	b_m	b_{m-1}	....	b_3	b_2	b_1	b_0	0	0	0	0
$m+3$	0	0	b_m	....	b_4	b_3	b_2	b_1	b_0	0	0	0
⋮												
$m+n-1$	0	0	0	0	b_m	b_{m-1}	b_{m-2}	....	b_2	b_1	b_0	0
$m+n$	0	0	0	0	0	b_m	b_{m-1}	....	b_3	b_2	b_1	b_0

Bezeichnet man nämlich die in der $k$ten Horizontalreihe und in der $i_k$ten Verticalreihe stehende Gröfse mit $\binom{k}{i_k}$

und läfst $i_1, i_2, \ldots. i_{m+n}$ die Zahlen $1, 2, 3, \ldots. m+n$ in beliebiger Reihenfolge bedeuten, so ist ein beliebiges Glied der Determinante das Product

$$\binom{1}{i_1}\cdot\binom{2}{i_2}\cdot\binom{3}{i_3}\cdots\binom{m+n}{i_{m+n}}.$$

Aus diesem Gliede erhält man durch alle möglichen Permutationen der untern Zahlen $i_1, i_2, \ldots. i_{m+n}$ alle Glieder der Determinante; wobei man jedem Gliede das positive oder negative Zeichen zu geben hat, je nachdem die entsprechende Permutation eine positive oder eine negative ist (welche Benennung durch die Abhandlung des Hrn. Prof. *Jacobi* über die Determinanten Bd. 22. genugsam bekannt ist).

Aus dieser Bildungsweise der Gleichung $P=0$ ist ersichtlich, dafs dieselbe in Rücksicht auf die Coëfficienten $a_n \ldots. a_0$ den Grad m, in Rücksicht auf die Coëfficienten $b_m \ldots. b_0$ den Grad n, endlich in Rücksicht auf sämmtliche Coëfficienten den Grad $m+n$ erreicht. Nun weiset aber *Euler* in den Memoiren der Berl. Akad. Tom. IV. an. 1748 pag. 234 etc. nach, dafs die Endgleichung, wenn sie keinen überflüssigen Factor enthält, in Rücksicht auf alle Coëfficienten der gegebenen Gleichungen vom Grade $m+n$ ist. Mithin enthält unsere Gleichung $P=0$ keinen überflüssigen Factor.

Nehmen wir nun an, die Coëfficienten a_p und b_p seien Functionen einer zweiten Variabeln, und bezeichnen der Kürze wegen durch dieselben Buchstaben a_p und b_p respective die Grade dieser Functionen, so wird der Grad des beliebigen, oben angegebenen Gliedes in P durch die Summe ausgedrückt werden:

$$\binom{1}{i_1}+\binom{2}{i_2}+\binom{3}{i_3}+\cdots\binom{m+n}{i_{m+n}}.$$

Da aber das Glied vom höchsten Grade zugleich den Grad der Gleichung bestimmt, so wird das Maximum der genannten Summe für die verschiedenen Permutationen der untern Zahlen den Grad der Endgleichung ergeben.

Über die Bestimmung der symmetrischen Functionen der Wurzeln einer gegebenen algebraischen Gleichung.

Irgend ein Glied einer gegebenen ganzen rationalen Function U vom $p$ten Grade der n Wurzeln $x_1, x_2, \ldots. x_n$ der Gleichung $A_0=0$ läfst sich in der Form

$$c.x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}\ldots. x_n^{\alpha_n}$$

darstellen, wo die Exponenten $\alpha_1, \alpha_3, \ldots. \alpha_n$ irgend welche gleiche oder un-

gleiche unter den Zahlen 1, 2, 3, ... p bedeuten; unter der Voraussetzung, dafs $\alpha_1+\alpha_2\ldots\alpha_n \leqq p$ sei. Der von den Wurzeln unabhängige Coëfficient c dieses Gliedes möge der Bequemlichkeit wegen durch

$$(\alpha_1\alpha_2\alpha_3\ldots\alpha_n)$$

bezeichnet werden, worauf dann das aus der symmetrischen Function U herausgehobene Glied die Form

$$(\alpha_1\alpha_2\ldots\alpha_n)\,x_1^{\alpha_1}\,x_2^{\alpha_2}\ldots x_n^{\alpha_n}$$

erhält. Die Natur der symmetrischen Function verlangt aber, dafs in ihr *alle verschiedenen* Glieder vorkommen, welche durch die Permutation der Wurzeln x_1, x_2, ... x_n miteinander aus diesem Gliede entstehen. Die Summe dieser Glieder wollen wir durch

$$(\alpha_1\alpha_2\ldots\alpha_n)\,\Sigma\,x_1^{\alpha_1}\,x_2^{\alpha_2}\ldots x_n^{\alpha_n},$$

oder kürzer durch

$$(\alpha_1\alpha_2\ldots\alpha_n)\,[\alpha_1\alpha_2\ldots\alpha_n]$$

bezeichnen. Unter dieser Voraussetzung kann die symmetrische Function U als die Summe der Glieder $(\alpha_1\alpha_2\ldots\alpha_n)[\alpha_1\alpha_2\ldots\alpha_n]$ dargestellt werden, indem man für α_1, α_2, ... α_n alle gleichen und ungleichen Zahlen 1, 2, ... p setzt; unter der Beschränkung, dafs die Summe $\alpha_1+\alpha_2+\ldots\alpha_n$ die Zahl p nicht übersteigen dürfe. Demnach haben wir:

$$U = \Sigma(\alpha_1\alpha_2\ldots\alpha_n)[\alpha_1\alpha_2\ldots\alpha_n].$$

Nehmen wir an, q sei eine ganze Zahl, kleiner als p, so wird unter der Bedingung

$$\alpha_1+\alpha_2+\ldots\alpha_n = q$$

jene Function U homogen und vom $q$ten Grade sein.

Da eine beliebige symmetrische Function der Wurzeln auf die genannte Weise aus den einfachen symmetrischen Functionen

$$[\alpha_1\alpha_2\ldots\alpha_n]$$

zusammengesetzt werden kann, so wollen wir letztere die Elemente der symmetrischen Function nennen. Wir werden nun zeigen, wie diese Elemente durch die Coëfficienten der gegebenen Gleichung $A_0=0$ ausgedrückt werden können.

Euler gelangt an dem oben angegebenen Orte zu der durch Elimination von x aus den Gleichungen $A_0=0$, $B_0=0$ (welche wir jetzt durch $f(x)=0$ und $\varphi(x)=0$ bezeichnen wollen) hervorgehenden Endgleichung, indem er die Wurzeln der ersten Gleichung x_1, x_2, ... x_n nach einander in die zweite setzt; wodurch sich n Gleichungen ergeben, deren Product

$$\varphi(x_1).\varphi(x_2)\ldots\varphi(x_n) = 0$$

die gesuchte Endgleichung wird, wenn man den linken Theil der Gleichung nach den verschiedenen Producten der Coëfficienten b_m, b_{m-1}, ... b_0 der

zweiten Gleichung entwickelt und die symmetrischen Functionen der Wurzeln $x_1, x_2, \dots x_n$, mit welchen jene Producte multiplicirt sind, durch die Coëfficienten der ersten Gleichung ausdrückt. Ein beliebiges Glied der Entwicklung jenes Products ist von der Form:

$$b_{\alpha_1}.b_{\alpha_2}\dots b_{\alpha_n}[\alpha_1\alpha_2\dots\alpha_n],$$

und die Gleichung selbst ist

$$\Sigma\, b_{\alpha_1}.b_{\alpha_2}\dots b_{\alpha_n}[\alpha_1\alpha_2\dots\alpha_n] = 0;$$

wo $\alpha_1, \alpha_2, \dots \alpha_n$ die Zahlen $1, 2, \dots m$, gleiche oder ungleiche, bedeuten. Man erhält also die Endgleichung, wenn man die Elemente $[\alpha_1\alpha_2\dots\alpha_n]$ der symmetrischen Function durch die Coëfficienten der Gleichung $f(x)=0$ ausdrückt und in die angegebene Gleichung substituirt. Die Bildung dieser Ausdrücke der Elemente macht aber gröfsere Schwierigkeit, als die angegebene Bildung der Endgleichung $P=0$. Man wird es daher vorziehen, umgekehrt durch die Endgleichung die Elemente der symmetrischen Functionen zu bestimmen.

Die durch die Elimination von x aus den Gleichungen $f(x)=0$ und $\varphi(x)=0$ hervorgehende Endgleichung ist sowohl

$$\Sigma\, b_{\alpha_1} b_{\alpha_2}\dots b_{\alpha_n}[\alpha_1\alpha_2\dots\alpha_n] = 0, \quad \text{als} \quad P = 0,$$

deren linken Theile, wenn man die Coëfficienten $b_m, b_{m-1}, \dots b_0$ der Gleichung $\varphi(x)=0$ als variabel betrachtet, abgesehen von einem constanten Factor, gleich sein müssen. Nun ist aber in dem linken Theile der ersten Gleichung der Coëfficient von b_0^n gleich $[0\,0\dots 0]=1$. Dividiren wir daher P durch den Coëfficienten von b_0^n, welchen diese Potenz in der Entwicklung von P hat, und den wir mit δ bezeichnen wollen, so wird

$$\Sigma\, b_{\alpha_1} b_{\alpha_2}\dots b_{\alpha_n}[\alpha_1\alpha_2\dots\alpha_n] = \frac{P}{\delta};$$

aus welcher Gleichung durch Gleichstellung der Coëfficienten gleicher Producte der Variabeln $b_m, b_{m-1}, \dots b_0$ die Elemente der symmetrischen Functionen der gegebenen Gleichung $f(x)=0$ sich als Functionen der Coëfficienten dieser Gleichung ergeben.

Will man auf diese Weise sämmtliche Elemente einer symmetrischen Function vom $p$ten Grade bestimmen, so wird man, um unnöthige Rechnungen zu vermeiden, m, welches den Grad der Gleichung $\varphi(x)=0$ angiebt, und über welches man nach Belieben verfügen kann, gleich p setzen. Unter dieser Voraussetzung, oder auch wenn $m>p$ ist, geht der Ausdruck $\frac{P}{\delta}$, wenn man in der Entwicklung desselben nach den verschiedenen Producten der Coëfficienten $b_m, b_{m-1}, \dots b_0$ statt der Producte $b_{\alpha_1}, b_{\alpha_2}, \dots b_{\alpha_n}$, 0 oder $(\alpha_1\alpha_2\dots\alpha_n)$ setzt, je nachdem die Summe $\alpha_1+\alpha_2+\dots\alpha_n$ die Zahl p übersteigt, oder nicht, in den Werth der symmetrischen Function U über.

Königsberg, den 2ten October 1843.

2.

Encyklopädische und elementare Darstellung der Theorie der Zahlen.

(Vom Herausgeber dieses Journals.)

Vorbemerkung.

Das hier Folgende ist ein Versuch eines *elementaren* Vortrages der *Theorie der Zahlen*, und für den öffentlichen und Selbst-Unterricht bestimmt. Da die Zahlenlehre wegen der Mannigfaltigkeit und Eigenthümlichkeit der Beweise und der Verbindung ihrer Sätze, so wie, weil sie, anders wie die übrigen Theile der Mathematik, für sich selbst keiner Postulate und Axiome bedarf, folglich die vollkommenste Strenge und Gewifsheit besitzt, ja vielleicht in dem gesammten Bereich der menschlichen Erkenntnisse allein Dasjenige ist, was innerhalb seines Umfanges *vollkommene* Sicherheit hat, ganz besonders zur Entwicklung und Übung der jugendlichen Denkkraft und zur Gewöhnung an strenge Wahrheit, was einen Haupttheil der Zwecke des Unterrichts in der Mathematik ausmachen dürfte, sich eignet: so ist es in der That zu verwundern, und zu bedauern, dafs bis jetzt diese Theorie noch so wenig für den Unterricht der Jugend benutzt wurde und noch so wenig davon in die Lehrbücher überging. Das hier Folgende ist ein Versuch, sie so darzustellen, dafs sie dem Unterrichte zugänglich und für die Lehrbücher, in so weit sie sie aufnehmen wollen und ihrem Umfange nach aufnehmen können, benutzbar sein möge.

Dafs der Herausgeber diesen seinen Versuch in das gegenwärtige *Journal* aufnimmt, könnte Anstofs finden, indem dieses Journal, in der langen Reihe seiner Bände, durch die Beiträge, mit welchen es beehrt worden ist, den Anschein gewonnen hat, als widme es sich nur mehr dem sogenannten Höheren und Neuen, oder doch Weniger-bekannten; was gleichwohl nicht in seinen ursprünglichen Plane lag. Indessen ist auch das Höhere und Höchste eigentlich nichts Anderes als das Elementare, sobald es nur vollständig auseinandergesetzt und deutlich vorgetragen wird. Auch kommt selbst nicht die *Leichtigkeit* dem Elementaren ausschliefslich zu, sondern das Höhere ist ebenfalls leicht und unterscheidet sich von den Anfängen blofs dadurch, dafs dazu eine

mehr oder weniger grofse *Menge* von ursprünglichen Sätzen mit einander verbunden ist: denn alles, was wahr ist, ist auch klar; und alles, was klar ist, ist auch elementar und leicht, oder läfst sich wenigstens dazu machen. In diesem Sinne ist das Elementare dem Journale keinesweges fremd. Wäre aber etwa die weniger-allgemeine Verbreitetheit oder die Neuheit der Gegenstände eine Bedingung für die Aufnahme in das Journal, so läfst sich wohl sagen, dafs die Zahlentheorie bis jetzt nicht eben allgemein verbreitet ist; und an *Neuem* wird es in Dem, was hier folgt, nicht ganz fehlen. Schon die Absicht, die Zahlenlehre elementar darzustellen, ist neu; die Art der Darstellung dürfte es häufig ebenfalls sein; und *wahrscheinlich* sind es auch mehrere Entwicklungen und Beweise der Sätze. Selbst an neuen *Sätzen* wird es nicht ganz fehlen. Also wird wohl auch in dieser Beziehung die Aufnahme in das Journal nicht ganz unpassend sein. Der Herausgeber hat nicht das Vorhandene blofs verarbeitet und gleichsam nur in seine Darstellungsart übersetzt, sondern er hat das Meiste nach seiner eigenen Ansicht selbst entwickelt. Deshalb kann er denn auch nur sagen: *wahrscheinlich* sei Einiges neu. Er macht indessen für Dieses wiederum durchaus keinen Erfindungs-Anspruch, oder Ansprüche auf Priorität, sondern will es im voraus gern und willig zugeben, dafs *Alles,* was er vorträgt, auch von Andern schon gedacht und sogar gesagt sein mag. Wahrheiten sind ein Gemeingut, und für sie selbst ist es gleich, wer sie fand.

Dafs der Herausgeber die Sätze der Zahlenlehre, wie man sehen wird, nicht in gröfsere und kleinere *Abschnitte* gebracht hat, sondern sie nur nach der einzigen Regel auf einander hat folgen lassen, dafs kein Satz eher auftrete, ehe er nicht durch die vorhergehenden begründet werden kann, geschah aus folgenden Ursachen. Zuerst hält er ein wirkliches, nach innerer Nothwendigkeit angeordnetes System, bei dem gegenwärtigen, noch wenig abgeschlossenen Zustande dieser Theorie noch nicht für möglich. Sodann schien ihm die von ihm gewählte Form gerade für den besondern Zweck des Gebrauchs beim *Unterricht* die passendste, indem nun der Lehrer oder der Lernende einzelne Sätze herausnehmen kann und nur diese, nebst den darin angezeigten, auf welche sie sich gründen, durchzugehen braucht; auf welche stückweise Benutzung sich auch besonders der *öffentliche* Unterricht immer wird beschränken müssen, da die *gesammte* Theorie für denselben viel zu ausgedehnt ist. Endlich aber konnte er in seinen persönlichen Verhältnissen das Vorzutragende nur in *dieser* Form liefern, da er, im vorgerückten Alter, und seiner gänzlich zerstörten Gesundheit wegen, der Vollendung der Unter-

nehmung zu wenig sicher ist, in der gegenwärtigen Form es aber für Das was geliefert wurde keinen wesentlichen Nachtheil hat, wenn der Cursus des Vortrages auch *nicht* vollendet wird.

Dafs der Herausgeber auch Sätze aufnahm, die man gewöhnlich *nicht* zur Zahlentheorie rechnet, wird dadurch entschuldigt werden, dafs es *nur* da geschah, wo ihm die gewohnten und gangbaren Ansichten und Beweise nicht genügten.

Dafs er zum Theil *Zeichen* sich bedient, welche von den gebräuchlichen abweichen, darf nicht durch Worte entschuldigt werden, sondern mufs und wird auch hoffentlich sich durch sich selbst rechtfertigen.

Dafs er endlich zu den *Benennungen*, wie man finden wird, möglichst *deutsche* statt fremder Worte nahm, wird bei denjenigen Deutschen, die nicht fremde Sprachen höher schätzen, als ihre eigene, keiner Entschuldigung bedürfen. Man wolle ihn aber, und wird ihn auch wohl für das Wenige, was er in diesem Punct versuchte, nicht etwa zu den *Puristen*, wie man sie im *Deutschen* nennt, zählen. Nach seiner Meinung stiften diese Puristen, die mit der Bemühung um Reinigung der Sprache (welche ja, wie die Erfahrung lehrt, von selbst erfolgt, indem sie seit 50 und 100 Jahren bekanntlich schon gar sehr fortgeschritten ist) zu sehr der Zeit vorgreifen, der Sprache und durch sie den Wissenschaften eben so wenig Nutzen, wie Diejenigen, welche der Reinigung der Sprache widerstreben, oder doch sie als unnütz betrachten.

Der Herausgeber wünscht Dem was hier folgt eine geneigte und freundliche Aufnahme und die Anerkennung der guten *Absicht*. Er bittet die Leser des Journals, und die Jugendlehrer insbesondere, dem hier Folgenden selbige gewähren und sich für die *Benutzung* des Vorgetragenen interessiren zu wollen.

Berlin, im December 1843.

---

§. 1.

Erklärung und Erläuterung.

Das Zeichen $\times$, oder auch ein *Punct*, zwischen die Buchstaben gesetzt, welche Zahlengröfsen bezeichnen, soll anzeigen, dafs das Ergebnifs alles Dessen, was dem Zeichen vorhergeht, mit dem Ergebnifs alles Dessen, was ihm bis *zum nächsten Zeichen* folgt, zu *multipliciren* sei. Das *Ergebnifs* von Multiplicationen dagegen soll durch blofses *Aneinanderreihen* der Buchstaben, ohne dazwischen stehende Zeichen, ausgedrückt werden.

Also soll z. B. $a.b.c.d.e$ oder $a\times b\times c\times d\times e$ bezeichnen, dafs zunächst die Zahl a mit der Zahl b, die daraus hervorgehende Zahl mit der Zahl c, die hieraus hervorgehende Zahl mit der Zahl d u. s. w. zu multipliciren sei. Dagegen soll $abcde$ die Zahl bezeichnen, welche das letzte Ergebnifs dieser Multiplicationen ist.

Da auf solche Weise ab das Ergebnifs der durch $a.b$, $a.b.c$ das Ergebnifs der durch $a.b.c$ *angedeuteten* Multiplicationen ist u. s. w., so folgt *aus der blofsen Bedeutung der Zeichen*, dafs z. B. die Zahl $abcde$ auf folgende verschiedene Arten geschrieben werden kann:

1. $\quad abcde = abcd.e = abc.d.e = ab.c.d.e = a.b.c.d.e.$

Aber es folgt nicht eben so, ohne weitern Beweis, dafs auch z. B.

$$abcde = abc.de = ab.cde = ab.cd.e = a.bcde \text{ u. s. w.}$$

sei. Die Gründe dieser letzteren Gleichheit liegen *nicht* in der blofsen Bedeutung der Zeichen.

§. 2.

Lehrsatz.

Das Product

1. $\quad P_\nu = (1+a)(1+b)(1+c)(1+d)\dots(1+m)(1+n),$

in welchem a, b, c, d, ... m, n *beliebige ungleiche Zahlgröfsen sind, deren Anzahl durch* ν *bezeichnet werden mag, ist gleich der Summe der Einheit und aller möglichen ungleichen Producte von* a, b, c, ... m, n, *zu einem, zwei, drei, vier bis zu* ν *ungleichen Factoren, jeden Factor nur einmal genommen. Keines dieser Producte fehlt, und keines kommt mehr als einmal vor. Als ungleich werden alle diejenigen*

Producte betrachtet, von welchen nicht sämmtliche Factoren die nemlichen sind, in welcher Ordnung sie auch sonst auf einander folgen mögen.

Beispiel. Für die 5 Zahlengröfsen a, b, c, d und e ist

$$2.\quad (1+a)(1+b)(1+c)(1+d)(1+e)$$

$$\begin{aligned} = \; & 1 \\ & +a+b+c+d+e \\ & +ab+ac+bc+ad+bd+cd+ae+be+ce+de \\ & +abc+abd+acd+bcd+abe+ace+bce+ade+bde+cde \\ & +abcd+abce+abde+acde+bcde \\ & +abcde. \end{aligned}$$

Die Glieder rechts sind hier, aufser der Einheit, *alle möglichen* Producte von *einem, zwei, drei, vier* und *fünf ungleichen* Factoren. Keins fehlt, und keins, desgleichen auch kein Factor, kommt mehr als einmal vor.

Beweis. *A.* Anstatt zu beweisen, dafs das Product $P_{,} = (1+a)(1+b)(1+c)\ldots.(1+n)$ (1.) die Summe der Einheit und aller möglichen Producte von $a, b, c, \ldots. m, n$ zu einem, zwei, drei u. s. w. Factoren sei, werde, umgekehrt, bewiesen, dafs die ebengenannte Summe nichts anderes ist, als jenes Product. Daraus wird unmittelbar die Behauptung des Lehrsatzes folgen; denn wenn bewiesen ist, dafs eine Gröfse B einer Gröfse A gleich sei, so folgt auch, dafs nothwendig A gleich B ist.

B. Man nehme einen Augenblick an, die *rechts* in (2.) stehenden Producte seien wirklich *alle möglichen* aus den 5 Factoren a, b, c, d und e, zu *keinem* (was die 1 giebt), zu *einem, zwei, drei, vier* und *fünfen*, von welcher letzten Art offenbar nur das eine Product $abcde$ möglich ist, und es komme nun eine neue *sechste* Gröfse f hinzu.

Unstreitig befinden sich dann unter allen möglichen Producten der sechs Gröfsen a, b, c, d, e und f auch die der fünf Gröfsen a, b, c, d und e. Es sind unter jenen alle diejenigen, die den Factor f *nicht* enthalten, also gerade alle die, welche rechts in (2.) schon vorhanden sind; denn diese Producte sind nach der Voraussetzung *alle möglichen* aus den 5 Gröfsen a, b, c, d und e, *ohne* Rücksicht auf die sechste Gröfse f.

Um daher *alle möglichen* Producte aus den 6 Gröfsen a, b, c, d, e und f zu finden, kommt es nur darauf an, zu allen jenen möglichen Producten aus den 5 Gröfsen a, b, c, d und e noch alle die möglichen Producte hinzuzuthun, welche von der sechsten Gröfse f herrühren; also diejenigen, welche sämmtlich f zum *Factor* haben.



C. Diese ergeben sich wie folgt.

Zu der *zweiten* horizontalen Zeile nemlich rechts in (2.), welche blofs Producte von *einem* Factor enthält, kommt offenbar nur f selbst hinzu; denn es giebt kein anderes Product mit dem *einen* Factor f. Also ist zu der *zweiten* Zeile noch f, multiplicirt mit der 1 aus der *ersten* Zeile, hinzuzuthun.

Was zu der *dritten* horizontalen Zeile rechts in (2.), die nach der Voraussetzung alle möglichen Producte von zwei Factoren aus den 5 Gröfsen a. b, c, d und e enthält, wegen f noch hinzukommt, findet sich, wenn man *alle möglichen* Producte von *einem Factor* aus den 5 Gröfsen a, b, c, d, e mit f multiplicirt; denn dies giebt offenbar *alle die möglichen* Producte von *zwei* Factoren, deren jedes f zu einem seiner Factoren hat. Alle möglichen Producte von einem Factor stehen aber in der *zweiten* Zeile, also mufs man diese ganze zweite Zeile mit f multipliciren und das Resultat zu der *dritten* hinzuthun. Alsdann enthält die dritte Zeile *alle möglichen* Producte von zwei Factoren aus den 6 Gröfsen a, b, c, d, e und f.

Eben so findet sich, was zu der *vierten* horizontalen Zeile rechts in (2.), die nach der Voraussetzung alle möglichen Producte von *drei* Factoren aus den 5 Gröfsen a, b, c, d und e enthält, wegen f noch hinzukommt, wenn man *alle möglichen* Producte von *zwei* Factoren aus den 5 Gröfsen a, b, c. d und e mit f multiplicirt; denn das giebt offenbar alle die *möglichen* Producte von *drei* Factoren, deren jeder f zu einem seiner Factoren hat. Alle die möglichen Producte von 2 Factoren stehen aber in der *dritten* Zeile: also mufs man diese ganze dritte Zeile mit f multipliciren und das Resultat zu der *vierten* hinzuthun. Alsdann enthält diese vierte Zeile *alle möglichen* Producte von drei Factoren aus den 6 Gröfsen a, b, c, d, e und f.

Gleicherweise verhält es sich mit den folgenden Zeilen. Man mufs die ganze *vierte* Zeile mit f multipliciren und das Resultat zur *fünften* hinzuthun, worauf diese alle möglichen Producte von vier Factoren aus den 6 Gröfsen a, b, c, d, e und f enthält. Und so weiter.

Zuletzt kommt durch das eine mögliche Product $abcdef$ *aller* 6 Gröfsen a, b, c, d, e und f eine neue 7te Zeile hinzu, die aber gleichmäfsig entsteht, wenn man die 6te Zeile, die nur das eine, aus den 5 Gröfsen a, b, c, d und e mögliche Product von 5 Factoren enthält, noch mit f multiplicirt.

D. Um daher *alle möglichen* Producte, von keinem, einem, zwei, drei u. s. w. Factoren aus *sechs* Gröfsen aus der Gesammtheit aller möglichen Producte von keinem, einem, zwei, drei u. s. w. Factoren aus *fünf* Gröfsen zu

2 *

finden, ist nichts weiter nöthig, als ***jede*** Zeile der letzteren, folglich die ***Gesammtheit*** derselben, mit der neuen sechsten Gröfse f zu multipliciren und das Resultat zu der Gesammtheit der Producte aus 5 Gröfsen hinzuzuthun.

E. Ob nun aber gerade 5 Gröfsen, wie in dem Beispiel, zuerst vorhanden sind, und eine neue sechste hinzukommt, oder ob anfangs weniger oder mehr Gröfsen vorhanden sind, ändert offenbar an dem Obigen nichts. Welche Zahl von Gröfsen auch zuerst vorhanden sein mag: immer ist, um aus der Gesammtheit der Producte von keinem, einem, zwei, drei u. s. w. Factoren aus ihrer Mitte die Gesammtheit der Producte für ***eine Gröfse mehr*** zu finden, nichts weiter nöthig, als die schon vorhandenen Producte sämmtlich noch mit der ***neuen*** Gröfse zu multipliciren und das Resultat zu den vorhandenen Producten hinzuzuthun.

F. Wären also ursprünglich statt der 5 Gröfsen a, b, c, d, e allgemein die $\nu-1$ Gröfsen $a, b, c, d, \ldots. m$ vorhanden, bezeichnete man die Gesammtheit ***aller möglichen*** Summen ihrer Producte von keinem, einem, zwei, drei u. s. w. Factoren durch $S_{\nu-1}$, und käme nun eine neue, νte Gröfse n hinzu, so würde die Gesammtheit oder die Summe ***aller möglichen*** Producte von keinem, einem, zwei, drei etc. Factoren aus den ν Gröfsen $a, b, c, d, \ldots. n$, welche S_ν ausdrückt, gefunden werden, wenn man $S_{\nu-1}$ mit n multiplicirt und das Resultat noch zu $S_{\nu-1}$ hinzuthut. Also würde

$$3.\quad S_\nu = S_{\nu-1} + n\,.\,S_{\nu-1} = (n+1)S_{\nu-1}$$

sein.

G. Was aber für ν gilt, gilt auch zufolge (**E.**) für $\nu-1$, oder für den Fall, wenn ursprünglich nur die $\nu-2$ Gröfsen $a, b, c, d, \ldots. l$ vorhanden wären und die $\nu-1$te neue Gröfse m hinzukäme. Also ist vermöge (3.) auch

$$4.\quad S_{\nu-1} = (m+1)S_{\nu-2},$$

und dies, in (3.) gesetzt, giebt

$$5.\quad S_\nu = (m+1)(n+1)S_{\nu-2}.$$

Eben so gilt, was für $\nu-1$ gilt, auch für $\nu-2$, oder für den Fall, wenn ursprünglich nur $\nu-3$ Gröfsen $a, b, c, d, \ldots. k$ vorhanden wären und es käme die $\nu-2$te neue Gröfse l hinzu. Also ist vermöge (3.) auch

$$6.\quad S_{\nu-2} = (l+1)S_{\nu-3},$$

und dies, in (5.) gesetzt, giebt

$$7.\quad S_\nu = (l+1)(m+1)(n+1)S_{\nu-3}.$$

H. So findet sich weiter

$$8. \quad \begin{cases} S_\nu = (k+1)(l+1)(m+1)(n+1)S_{\nu-4}, \\ S_\nu = (i+1)(k+1)(l+1)(m+1)(n+1)S_{\nu-5}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

und zuletzt

$$9. \quad S_\nu = (n+1)(m+1)(l+1)(k+1) \ldots\ldots (b+1)S_1.$$

I. Aber die Gesammtheit oder die Summe S_1 der Producte für *blofs eine* Gröfse a, welche S_1 bezeichnet, ist offenbar $1+a$; denn aufser der Einheit giebt es aus blofs einer Gröfse a kein anderes Product als a selbst. Also ist schliefslich

$$10. \quad S_\nu = (1+a)(1+b)(1+c)(1+d) \ldots\ldots (1+m)(1+n).$$

K. Es findet sich also, dafs die Gesammtheit oder die Summe S_ν *aller möglichen* Producte von keinem, einem, zwei, drei etc. Factoren aus den ν Gröfsen $a, b, c, d, \ldots\ldots n$, so genommen, dafs keines mehr als einmal vorhanden ist, und keines fehlt, auch keine Gröfse mehr denn einmal als Factor vorkommt, durch das ***Product*** P_ν (1.) der ν Gröfsen $1+a$, $1+b$, $1+c$, ... $1+n$ ausgedrückt wird. Mithin ist auch umgekehrt das Product P_ν *dieser* Gröfsen gleich der Gesammtheit S_ν aller möglichen Producte von keinem, einem, zweien, dreien etc. aus den ν Gröfsen $a, b, c, d, \ldots\ldots n$.

L. Anm. Das Hauptmoment des Beweises ist, dafs aus der Gesammtheit aller möglichen Producte von keinem, einem, zwei, drei etc. Factoren einer beliebigen Zahl von Gröfsen $a, b, c, d, \ldots\ldots$ die Gesammtheit der Producte für *eine Gröfse mehr* gefunden wird, wenn man jene Gesammtheit mit der neuen Gröfse multiplicirt und das Resultat zu jener Gesammtheit hinzuthut.

§. 3.

Lehrsatz.

Die Anzahl aller möglichen Producte von einer, zwei, drei etc. bis zu ν aus ν beliebigen Gröfsen oder Zahlen a, b, c, d, ... m, n *ist, wenn man noch die Einheit, diese gleichsam als Product keines jener Factoren, hinzuthut, gleich* 2^ν.

Beispiel. Für 5 Zahlen a, b, c, d und e sind folgende Producte möglich.

1.
- Das 1 Product mit keinem Factor, 1.
- Die 5 Producte von 1 Factor, nemlich *a, b, c, d, e*.
- Die 10 Producte von 2 Factoren, nemlich *ab, ac, ad, ae, bc, bd be, cd, ce, de*.
- Die 10 Producte von 3 Factoren, nemlich *abc, abd, abe, acd, ace, ade, bcd, bce, bde, cde*.
- Die 5 Producte von 4 Factoren, nemlich *abcd, abce, abde, acde, bcde*
- Das 1 Product von 5 Factoren, nemlich *abcde*.

Thut zusammen 32 Producte, und für $\nu = 5$, wie hier, ist $2^\nu = 2^5 = 32$.

Beweis. Zufolge (§. 2.) enthält das Product

$$2. \quad P_\nu = (1+a)(1+b)(1+c)(1+d)\ldots(1+n),$$

wenn man es entwickelt, nächst der Einheit, *alle möglichen* Producte aus den ν Factoren $a, b, c, d, \ldots n$ zu einem, zwei, drei etc. bis ν; und keines dieser Producte mehr als einmal.

Für beliebig *bestimmte* Zahlenwerthe von $a, b, c, d, \ldots n$ findet man den *Zahlenwerth* des Products P_ν offenbar eben sowohl, wenn man den Buchstaben $a, b, c, d, \ldots n$ in (2.), als wenn man ihnen in den *einzelnen Gliedern* des *entwickelten* Products die ihnen bestimmten Zahlenwerthe beilegt; und zwar *immer, welche* auch die Zahlenwerthe von $a, b, c, d, \ldots n$ sein mögen.

Macht man nun z. B. $a = b = c = d \ldots = n = 1$, so ist der Zahlenwerth *jedes* Gliedes des *entwickelten* Products *gleich 1*, und folglich die *Summe* dieser Glieder, das heifst P_ν, ihrer *Anzahl* gleich. Andrerseits ist für $a = b = c = d \ldots = n = 1$, zufolge (2.), $P_\nu = (1+1)(1+1)(1+1)\ldots(1+1)$, oder, da P_ν ν Factoren hat, $= 2^\nu$; mithin ist die *Anzahl* der Glieder des entwickelten Products P_ν gleich 2^ν.

§. 4.

Lehrsatz.

Der Werth eines Products beliebiger ganzer Zahlen a, b, c, d, … … m, n, *deren Anzahl durch* ν *bezeichnet werden mag, bleibt derselbe, man mag erst* a *mit* b, *das Ergebnifs davon mit* c, *das Ergebnifs davon mit* d *u. s. w. multipliciren, oder man mag das Ergebnifs der Multiplication einiger ersten Factoren mit dem Ergebnifs der Multiplication einiger folgenden. u. s. w. bis zu Ende, multipliciren. Es wird indessen*

einstweilen vorausgesetzt, dafs bei der einen und der andern Art der Multiplicationen die Factoren in der gleichen Aufeinanderfolge in Rechnung kommen.

In dem Sinne der Bedeutung des Vorhandenseins oder der Abwesenheit des Puncts als Multiplicationszeichen (§. 1.), dafs nemlich das Vorhandensein des Puncts die Operation und die Abwesenheit desselben das Resultat derselben andeutet, behauptet der Lehrsatz, dafs z. B. in dem Product

$$1.\quad P_r = a.b.c.d.e \ldots . i.k.l.m.n$$

die Puncte, wo man will, und ihrer so viele, als man will, weggelassen werden können, ohne dafs der Werth des Products sich änderte.

Übrigens können die Zahlengröfsen a, b, c, d, ... n *unter einander sämmtlich ungleich, oder einige davon, oder alle können einander gleich sein. Der Satz bleibt derselbe.*

Beispiel. Es ist

$$2.\quad \begin{cases} 4.6.5.3.9 \\ = 4.6.5.27 = 4.6.15.9 = 4.30.3.9 = 24.5.3.9 \\ = 4.6.135 = 4.90.9 = 120.3.9 = 4.30.27 = 24.5.27 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = 24.15.9 \\ = 4.810 = 24.315 = 120.27 = 360.9 \\ = 3240. \end{cases}$$

In der ersten horizontalen Reihe (2.) ist *kein* Punct weggelassen; in der zweiten Zeile ist je *ein* Punct; in der dritten Zeile sind auf alle mögliche Weise *zwei* Puncte weggelassen; in der vierten Zeile *drei* Puncte, und in der fünften Zeile alle *vier* Puncte.

Beweis. *A.* Man bezeichne der Kürze wegen

$$3.\quad \begin{cases} a.b.c.d \ldots . i.k.l.m.n & \text{durch } P, \\ a.b.c.d \ldots . i.k.l.m & \text{durch } M, \\ a.b.c.d \ldots . i.k.l & \text{durch } L, \\ a.b.c.d \ldots . i.k & \text{durch } K, \\ a.b.c.d \ldots . i & \text{durch } I, \\ \text{u. s. w.}; \end{cases}$$

so dafs also, der Bedeutung (§. 1.) des Multiplicationspunctes gemäfs,

$$4.\quad \begin{cases} P = M.n = L.m.n = K.l.m.n = I.k.l.m.n, \\ M = L.m = K.l.m = I.k.l.m, \\ L = K.l = I.k.l, \\ K = I.k \end{cases}$$

u. s. w. ist.

B. Nun bedeutet der Ausdruck $L.m.n$ von P in der ersten Zeile (4.), dafs L erst m mal und dann das was herauskommt n mal genommen werden soll. Man schreibe L in einer horizontalen Zeile m mal neben einander, und n solcher Zeilen, nemlich:

$$5. \quad \left.\left\{\begin{array}{l} \overbrace{L, L, L, L, \ldots . L}^{m} \\ L, L, L, L, \ldots . L \\ L, L, L, L, \ldots . L \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ L, L, L, L, \ldots . L \end{array}\right.\right\} n,$$

so ist hier L wirklich erst m mal genommen, und dann das Ergebnifs n mal. Also stellt die *Gesammtheit* der L in (5.) P vor.

Aber die *Anzahl* der in (5.) vorhandenen L ist offenbar der *Zahl* mn gleich, denn es sind der L so viele vorhanden als das *Product* m mal n Einheiten hat, also mn. Folglich ist P auch nichts anderes als L, mn mal genommen, und folglich ist auch

$$6. \quad P = L.mn = a.b.c.d \ldots . i.k.l.mn,$$

und daraus folgt, dafs der Werth P sich nicht ändert, wenn man in seinem Ausdruck (1.) den *letzten* Punct wegläfst.

Wir haben also bis jetzt folgende *zwei* verschiedene Ausdrücke von P:

$$7. \quad \begin{cases} P = L.m.n & (4.) \text{ und} \\ P = L.mn & (6.). \end{cases}$$

C. Nun ist in diesen Ausdrücken L nichts anderes als $K.l$ (3.), also kann P vermöge (6.) auch wie folgt geschrieben werden:

$$8. \quad P = K.l.mn.$$

Es zeigte sich aber so eben, dafs, wenn eine Zahl L erst m, und dann das was herauskommt n mal genommen wird, das Ergebnifs das nemliche ist, als wenn man L sogleich mn mal nimmt. Also wird auch in (8.), wo die Zahl K erst mit l und dann das was herauskommt mit *der Zahl* mn multiplicirt werden soll, das Ergebnifs das nemliche sein, als wenn man K sogleich mit dem Product lmn der beiden *Zahlen* l und mn multiplicirt. Mithin ist auch

$$9. \quad P = K.lmn = a.b.c.d \ldots . i.k.lmn \quad (3.):$$

und daraus folgt, dafs der Werth von P sich wiederum nicht ändert, wenn man in seinem Ausdruck die *beiden* letzten Puncte wegläfst.

D. Gesetzt nun, es wäre K, statt wie in (8.) erst mit der Zahl l und dann das Ergebnifs mit der Zahl mn, vielmehr K erst mit der *Zahl* lm und dann das Resultat davon mit der *Zahl* n zu multipliciren, so würde das Ergebnifs, aus *gleichem* Grunde wie in (*C.*), $= K.lmn$ sein. Dieses aber ist $= P$ (9.). Also kann P auch durch

$$10. \quad P = K.lm.n = a.b.c.d \ldots . i.k.lm.n$$

ausgedrückt werden; und daraus folgt, dafs der Werth von P sich auch nicht verändert, wenn man in seinem Ausdruck (1.) den *vorletzten* Punct wegläfst. Es dürfen also in dem Ausdrucke von P (1.) sowohl die *beiden letzten* Puncte, nach (9.), als der letzte Punct, nach (8.), oder der vorletzte Punct, nach (10.), weggelassen werden, ohne den Werth von P zu ändern.

Demnach haben wir bis hierher folgende *vier* verschiedene Ausdrücke von P:

$$11. \quad \begin{cases} P = K.l.m.n & (4.), \\ P = K.l.mn & (8.), \\ P = K.lm.n & (10.), \\ P = K.lmn & (9.). \end{cases}$$

E. Man setze in diesen 4 Ausdrücken von P statt K seinen Werth $I.k$ (4.), so erhält man aus (11.) folgende *4 neue Ausdrücke* von P:

$$12. \quad P = I.k.l.m.n = I.k.l.mn = I.k.lm.n = I.k.lmn.$$

In die 2 Ausdrücke von P (7.) dagegen setze man aus (4.) den Werth $I.k.l$ von L, der auch, eben so wie zufolge $L.m.n = Lmn$, nichts anderes ist als $I.kl$, so erhält man noch folgende *2 Ausdrücke* von P:

$$13. \quad P = I.kl.m.n = I.kl.mn.$$

Man setze endlich in den Ausdruck $M.n$ von P (4.) den Werth $I.k.l.m$ von M, der aus demselben Grunde, aus welchem zufolge (*C.*) $K.l.m.n = K.lmn$ war, nichts anderes als $I.klm$ ist, so erhält man noch folgenden *1 Ausdruck* von P:

$$14. \quad P = I.klm.n,$$

und dieser Ausdruck giebt, aus demselben Grunde, aus welchem zufolge (*B.*) $L.m.n = L.mn$ war, endlich noch den *1 Ausdruck*

$$15. \quad P = I.klmn.$$

Zusammen also haben wir nun aus (12. 13. 14. und 15.) $4+2+1+1 = 8$ verschiedene Ausdrücke von P. Sie sind, wenn man sie so ordnet, wie in ihnen *keiner*, oder *einer*, oder *zwei*, oder *drei* Puncte zwischen k, l, m und n *fehlen*, folgende:

$$16.\quad \begin{cases} P = I.k.l.m.n \ (12.), \\ P = I.k.l.mn \ (12.) = I.k.lm.n \ (12.) = I.kl.m.n \ (13.), \\ P = I.k.lmn \ (12.) = I.kl.mn \ (13.) = I.klm.n \ (14.), \\ P = I.klmn \ (15.). \end{cases}$$

Keiner dieser Ausdrücke ist seiner *Form* nach dem andern gleich; denn die 4 Ausdrücke (12.) entstanden aus den 4 unter sich verschiedenen Ausdrücken (11.) durch Hinzuthun von k, *mit* einem Punct zwischen k und l; die 2 Ausdrücke (13.) entstanden aus den beiden unter sich verschiedenen Ausdrücken (7.), ebenfalls durch Hinzuthun von k, oder *ohne* Punct zwischen k und l, jedoch mit einem Punct zwischen l und m, und sind also durch das *Erste* von den vorigen wesentlich verschieden; der eine Ausdruck (14.) entstand aus (4.) durch Hinzuthun von k, l und m, *ohne* Punct zwischen k und l und l und m, aber *mit* einem Punct zwischen m und n, und ist also dadurch ebenfalls von allen vorigen verschieden. Der Ausdruck (15.) hat gar keinen Punct zwischen k, l, m und n, während alle vorigen wenigstens einen Punct hatten, und ist also ebenfalls von allen vorigen verschieden.

F: Man setze weiter in die 8 Ausdrücke von P (16.) den Werth $H.i$ von I. (4), so bekommt man *8 neue Ausdrücke* von P, die, eben wie die 8, aus welchen sie entstanden, unter sich verschieden sind, und sämmtlich zwischen i und k einen Punct haben. Es sind folgende:

$$17.\quad \begin{cases} P = H.i.k.l.m.n, \\ P = H.i.k.l.mn = H.i.k.lm.n = H.i.kl.m.n, \\ P = H.i.k.lmn = H.i.kl.mn = H.i.klm.n, \\ P = H.i.klmn. \end{cases}$$

In die 4 Ausdrücke von P (11.) setze man den Werth $H.i.k$ von K (4.), der zufolge (B.) nichts anderes ist als $H.ik$, so bekommt man *4 Ausdrücke* von P, die, eben wie die 4, aus welchen sie entstanden, *unter sich*, aber auch von den vorigen 8 *dadurch* verschieden sind, dafs sie sämmtlich, anders wie diese, zwischen i und k *keinen* Punct haben, wiewohl alle zwischen k und l einen Punct. Es sind folgende:

$$18.\quad \begin{cases} P = H.ik.l.m.n, \\ P = H.ik.l.mn = H.ik.lm.n, \\ P = H.ik.lmn. \end{cases}$$

In die 2 Ausdrücke (7.) von P setze man den Werth $H.i.k.l$ von L (4.), der zufolge (C.) nichts anderes ist als $H.ikl$, so bekommt man ferner *2 Ausdrücke* von P, die, eben wie die 2, aus welchen sie entstanden,

unter sich, aber auch von allen vorigen ***dadurch*** verschieden sind, dafs sie, anders wie diese, weder zwischen i und k, noch zwischen k und l einen Punct haben, wiewohl beide zwischen l und m einen Punct. Es sind folgende:

$$19.\quad \begin{cases} P = H.ikl.m.n \text{ und} \\ P = H.ikl.mn. \end{cases}$$

In den einen Ausdruck $P = M.n$ (4.) setze man den Werth $H.i.k.l.m$ von M, der zufolge (*E.*) nichts anderes ist als $H.iklm$, so erhält man

$$20.\quad P = H.iklm.n;$$

welcher Ausdruck wieder von allen vorigen dadurch ***verschieden*** ist, dafs er, anders wie sie, weder zwischen i und k, wie (17.), noch zwischen k und l, wie (18.), noch zwischen l und m, wie (19.), einen Punct hat, sondern nur noch zwischen m und n.

Endlich giebt (20.) vermöge (*B.*) noch den Ausdruck

$$21.\quad P = H.iklmn,$$

welcher wieder von allen vorigen ***dadurch*** verschieden ist, dafs er nirgend zwischen den Factoren i, k, l, m und n einen Punct hat.

Wir haben also nun zusammengenommen aus (17. 18. 19. 20. und 21.)

$$22.\quad 8+4+2+1+1 = 16$$

Ausdrücke von P, die ***alle*** unter einander ***verschieden*** sind. Sie sind, auf die Weise geordnet, wie zwischen i, k, l, m und n ***keiner***, oder ***einer***, oder ***zwei***, oder ***drei***, oder alle ***vier*** Puncte ***fehlen***, folgende:

$$23.\quad \begin{cases} P = H.i.k.l.m.n\ (17.) \\ P = H.i.k.l.mn\ (17.) = H.i.k.lm.n\ (17.) = H.i.kl.m.n\ (17.) \\ \qquad\qquad\qquad\qquad\qquad\qquad = H.ik.l.m.n\ (18.), \\ P = H.i.k.lmn\ (17.) = H.i.kl.mn\ (17.) = H.ik.l\,mn\ (18.) \\ \quad = H.i.klm.n\ (17.) = H.ik.lm.n\ (18.) = H.ikl.m.n\ (19.), \\ P = H.i.klmn\ (17.) = H.ik.lmn\ (18.) = H.ikl.mn\ (19.) \\ \qquad\qquad\qquad\qquad\qquad\qquad = H.iklm.n\ (20.), \\ P = H.iklmn\ (21.). \end{cases}$$

G. Verfährt man von Neuem ganz ähnlich wie in (*F.*), indem man nemlich in die 16 Ausdrücke von P (23.) statt H seinen Werth $G.h$, in die 8 Ausdrücke (16.) statt I seinen andern Ausdruck $G.hi$, in die 4 Ausdrücke (11.) statt K seinen dritten Ausdruck $G.hik$, in die 2 Ausdrücke (7.) statt L seinen vierten Ausdruck $G.hikl$ und in den 1 Ausdruck (4.) statt M seinen fünften Ausdruck $hiklm$ setzt, so bekommt man, mit $P = G.hiklm.n = G.hiklmn$ zusammengenommen,

$$24. \quad 16+8+4+2+1+1 = 32$$

Ausdrücke von P, die, aus ganz ähnlichen Gründen wie in (F.), alle von einander verschieden sind.

H. So also kommen, wenn man auf diese Weise weiter fortfährt, durch jede neue Operation immer gerade *ebensoviele neue*, unter sich und von den vorigen verschiedene Ausdrücke von P zum Vorschein, *als zusammengenommen bis dahin vorhanden waren.* Die Zahl der verschiedenen Ausdrücke von P wird also durch jede Substitution gerade *verdoppelt.*

Zuerst waren 2 Ausdrücke (7.) von P vorhanden. Durch die nächste Substitution stieg ihre Zahl auf das *Doppelte*, auf 4 (11.); durch die folgende Substitution wieder auf das *Doppelte*, auf 8 (16.); sodann abermals auf das *Doppelte*, auf 16 (23.) u. s. w. In den 2 Ausdrücken (7.) enthielt L noch $\nu-2$ Factoren; in den $4=2^2$ Ausdrücken (11.) enthielt K noch $\nu-3$ Factoren; in den $8=2^3$ Ausdrücken (16.) enthielt I noch $\nu-4$ Factoren; in den $16=2^4$ Ausdrücken (23.) enthielt H noch $\nu-5$ Factoren. Fährt man also so fort, bis A nur noch den *einen* $=(\nu-(\nu-1))$ Factor a enthält, das heifst, bis P, wie in (1.), *ganz* durch seine einzelnen Factoren ausgedrückt ist, so wird man $2^{\nu-1}$ Ausdrücke von P gefunden haben, die in der Form *sämmtlich* unter sich *verschieden* sind; und zwar *dadurch*, dafs ihnen entweder *keiner*, oder, hier oder dort, immer an verschiedenen Stellen, *einer*, oder *zwei*, oder *drei* u. s. w., oder *alle* Puncte fehlen.

I. Fragt man nun gegenseits, auf wievielerlei *Arten* in dem Ausdruck

$$25. \quad P_\nu = a.b.c.d....i.k.l.m.n \quad (1.)$$

von den $\nu-1$ Puncten zwischen den ν Factoren $a, b, c, d, \ldots. n$ *keiner*, oder *einer*, oder *zwei*, oder *drei* u. s. w. bis $\nu-1$ Puncte fehlen *können*, so ist diese Frage keine andere, als auf wievielerlei Arten sich $\nu-1$ *Dinge* zu 0, 1, 2, 3, ... $\nu-1$ *verbinden* lassen; etwa zu Producten, wenn sie Zahlen wären: denn die *Puncte* sind zwar nicht *an sich selbst* von einander verschieden, aber sie sind es durch ihre *Stellung;* und in Rücksicht auf *diese* können sie allerdings mit $\nu-1$ von einander *verschiedenen* Dingen, z. B. Zahlen oder Factoren, *verglichen* werden. In solchem Betracht ist also die Frage dieselbe, wie die, welches die Zahl der *verschiedenen* möglichen Producte von $\nu-1$ Factoren zu 0, 1, 2, 3, ... $\nu-1$ sei.

Diese Zahl ist zufolge des Lehrsatzes (§. 3.)

$$26. \quad = 2^{\nu-1}:$$

also ist auch die Zahl aller möglichen verschiedenen *Arten*, wie in dem Aus-

druck von P (25.) 0, 1, 2, 3, ... $\nu-1$ von den $\nu-1$ Puncten zwischen den ν Factoren $a, b, c, d, \ldots. n$ *weggelassen* werden können, $=2^{\nu-1}$.

Gerade soviele, durch Weglassung der Puncte *verschiedene* Ausdrücke von P wurden aber oben gefunden (*H.*), und es zeigte sich, dafs alle diese verschiedenen Ausdrücke von P denselben *Werth* haben. Also wurden *alle möglichen,* der Form nach verschiedenen Ausdrücke von P gefunden, und es folgt mithin, dafs der Werth von P sich nicht ändere, *welche* und *wieviele* Puncte man auch zwischen den Factoren weglassen möge; was zu beweisen war.

K. Da übrigens der Beweis von den *Werthen* der Factoren $a, b, c, d, \ldots. n$ gar nicht abhängt, so folgt auch, dafs es gleichgültig ist, ob die die Factoren unter einander ungleich oder gleich sind.

Anm. Die Hauptmomente des Beweises sind, erstlich, die auf der *Anschauung* beruhende Bemerkung in (*B.*), dafs der *letzte* Multiplicationspunct zwischen den Factoren weggelassen werden könne; sodann die Bemerkung in (*D.*), dafs, da z. B. $k.l.mn$, eben nach der vorigen Bemerkung, dasselbe geben würde, wie $k.lm.n$, nemlich beides $k.lmn$, auch der *vorletzte* Punct *statt* des letzten weggelassen werden könne; und dann endlich der Umstand, dafs die Zahl der sämmtlich unter einander verschiedenen Ausdrücke von P, die sich mit Hülfe der beiden vorigen Bemerkungen finden, wie es in (*H.* und *I.*) sich zeigt, gerade *eben so grofs* ist, als, zufolge des Lehrsatzes (§. 3.), die Zahl aller möglichen *Verbindungen* der $\nu-1$ Multiplicationspuncte zu *keinem, einem, zwei, drei* u. s. w. bis $\nu-1$.

§. 5.

Lehrsatz.

Es können ν Elemente (z. B. Buchstaben oder Zahlen)

$$1.\quad a, c, c, d, \ldots. m, n$$

auf

$$2.\quad \overset{\nu}{x} = 1.2.3.4.5\ldots.\nu,$$

und nicht mehr und nicht weniger Arten, die der Aufeinanderfolge nach verschieden sind, aneinandergereiht oder mit einander verbunden werden.

Beispiel. Die vier Buchstaben a, b, c, d können auf folgende verschiedene Arten nebeneinander gestellt werden:

$$3.\quad \begin{cases} abcd & acbd & bacd & bcad & cbad & cabd \\ abdc & adbc & badc & bdac & dabc & dbac \\ adcb & acdb & dacb & dcab & cadb & cdab \\ dbca & dcba & bdca & bcda & cdba & cbda. \end{cases}$$

ν ist hier 4. und die Zahl der verschiedenen Verbindungen ist, wie man sieht,

4. $24 = 1.2.3.4 = 1.2 \ldots . \nu$.

Erster Beweis. *A.* Man lasse irgend *einen* der ν Buchstaben a, b, c, d, ... n, z. B. n, weg, und stelle sich *alle möglichen*, der Aufeinanderfolge nach *verschiedenen* Verbindungen der *übrigen* $\nu - 1$ Buchstaben vor. Ihre Anzahl werde durch $\overset{\nu-1}{x}$ bezeichnet. Hängt man nun jeder dieser Verbindungen den einen weggelassenen Buchstaben noch an, so wird man $\overset{\nu-1}{x}$ sämmtlich der Aufeinanderfolge nach unter sich verschiedene Verbindungen haben, und es giebt ihrer nicht mehr und nicht weniger *von denen*, welche alle n zum *letzten* Buchstaben haben.

B. Aber statt n kann man auch *jeden andern* der ν Buchstaben erst weglassen, alle möglichen, der Aufeinanderfolge nach verschiedenen Verbindungen der *übrigen* machen, und dann diesen Verbindungen jedesmal den zuerst weggelassenen Buchstaben wieder anhängen. Dieses giebt für *jeden* Buchstaben, den man zuerst wegliefs, und dann wieder anhängte, $\overset{\nu-1}{x}$ unter sich verschiedene Verbindungen: nicht mehr und nicht weniger: also überhaupt, da ν Buchstaben vorhanden sind, und *jeder* der *letzte* sein kann, ν *Gruppen*, jede von $\overset{\nu-1}{x}$ Verbindungen: und alle diese Verbindungen sind unter sich verschieden, nicht allein die in jeder Gruppe unter sich, sondern auch die in den verschiedenen Gruppen, weil jede *Gruppe* einen *andern letzten* Buchstaben hat. Desgleichen sind nicht mehr und nicht weniger als ν *Gruppen* möglich, weil jede Gruppe nothwendig *einen* Buchstaben zu ihrem *letzten* hat.

Also sind überhaupt

$$5. \quad \nu . \overset{\nu-1}{x} = \overset{\nu}{x}$$

sämmtlich der Aufeinanderfolge nach verschiedene Verbindungen von ν Buchstaben möglich: nicht mehr und nicht weniger.

C. Was nun von der Zahl ν gilt, gilt auch von jeder andern Zahl der Elemente: also auch von den Zahlen $\nu - 1$, $\nu - 2$, $\nu - 3$, ... mithin der Reihe nach von den Zahlen 2, 3, 4, ... ν.

Für $\nu = 2$, also $\nu - 1 = 1$, ist aber offenbar $\overset{\nu-1}{x} = \overset{1}{x} = 1$: denn *ein* Element läfst sich nur auf $\overset{1}{x} = 1$ Art stellen. Setzt man daher in (5.) der Reihe nach 2, 3, 4, 5, ... ν statt ν, so ergiebt sich

$$6.\quad \begin{cases} 2.1 = \overset{2}{x}, \\ 3.\overset{2}{x} = 3.2 = \overset{3}{x}, \\ 4.\overset{3}{x} = 4.3.2 = \overset{4}{x}, \\ 5.\overset{4}{x} = 5.4.3.2 = \overset{5}{x}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \nu.(\nu-1)(\nu-2)(\nu-3) \ldots. 2 = 1.2.3.4.5 \ldots. \nu = \overset{\nu}{x}; \end{cases}$$

wie es der Lehrsatz behauptet.

Zweiter Beweis. ***D.*** Einer und derselben beliebigen Verbindung der $\nu-1$ Elemente $a, b, c, d, \ldots. m$ kann das νte Element n an ν und nicht an mehreren *verschiedenen Stellen* hinzugefügt werden; nemlich, erst *unmittelbar hinter* jedem der $\nu-1$ Elemente, und dann noch *vor* dem ersten. Die auf solche Weise aus *einer* der Verbindungen der $\nu-1$ Elemente entstehenden ν Verbindungen sind alle unter sich verschieden, denn jede hat n an einer *andern Stelle;* auch giebt es ihrer nicht mehrere.

E. Was nun von irgend einer der Verbindungen von $\nu-1$ Elementen gilt, gilt auch gleichmäfsig von *jeder* andern ihrer sämmtlichen Verbindungen, deren *Anzahl* durch $\overset{\nu-1}{x}$ bezeichnet wurde. Jede derselben giebt durch Hinzufügung des neuen, νten Elements n, ν unter sich verschiedene Verbindungen. Auch sind stets die aus den *verschiedenen* $\overset{\nu-1}{x}$ Verbindungen von $\nu-1$ Elementen hervorgehenden Verbindungen von ν Elementen von den vorigen verschieden; denn die $\overset{\nu-1}{x}$ Verbindungen von $\nu-1$ Elementen sind es *ehe* ihnen das neue Element n hinzugefügt wurde, also sind sie es auch noch *hernach,* da durch die Hinzufügung von n an der Aufeinanderfolge der $\nu-1$ Elemente $a, b, c, d, \ldots. m$ nichts geändert wird.

F. Die durch die Hinzufügung des νten Elements n entstehenden $\overset{\nu-1}{x}$ Gruppen, jede von ν Verbindungen, und folglich die entstehenden $\overset{\nu-1}{x}.\nu$ Verbindungen sind daher *sämmtlich* von einander verschieden. Auch giebt es *nicht mehrere* Verbindungen der ν Elemente; denn jeder der $\overset{\nu-1}{x}$ Verbindungen von $\nu-1$ Elementen kann das νte Element auf nicht mehr als ν Arten hinzugefügt werden (***D.***), und der Verbindungen von $\nu-1$ Elementen, welchen das νte Element hinzugefügt werden könnte, giebt es nach der *Voraussetzung* nicht mehr als $\overset{\nu-1}{x}$. Die erlangten Verbindungen von ν Elementen sind also

alle möglichen, deren Anzahl durch $\overset{\nu}{x}$ bezeichnet wurde: folglich ist

$$7. \quad \overset{\nu-1}{x}.\nu = \overset{\nu}{x}.$$

Dieses ist dieselbe Gleichung wie (5. in *B.*), da, wie aus (*B.* §. 4.) erhellet, zwei ganzzahlige Factoren verwechselt werden können, ohne dafs das Product sich änderte. Aus (7.) folgt das Übrige wie in (*C.*).

Anm. Der erste Beweis weiset nach, dafs die möglichen Verbindungen von ν Elementen aus ν Gruppen von $\overset{\nu-1}{x}$ verschiedenen Verbindungen von $\nu-1$ Elementen bestehen: der zweite, dafs sie aus $\overset{\nu-1}{x}$ Gruppen von ν verschiedenen Verbindungen von $\nu-1$ Elementen bestehen; welches die Gleichungen (5.) und (7.) giebt, die nach (*B.* §. 4.) Eines und Dasselbe bedeuten. Aus (5. u. 7.) folgt der Satz, wenn man der Reihe nach $\nu = 2, 3, 4, \ldots \nu$ setzt.

Übrigens ist zu Dem was weiter folgt *nur eine* der beiden Gleichungen (5. u. 7.) nöthig, also eigentlich noch nicht die Zuhülfenahme des in (*B.* §. 4.) sich ergebenden Satzes, dafs in einem Product von *zwei* Factoren die beiden Factoren *verwechselt* werden können.

§. 6.

Lehrsatz.

I. *Die Ordnung, in welcher die ungleichen oder gleichen ganzzahligen Factoren eines Products, z. B. die ν ganzzahligen Factoren* a, b, c, d, ... m, n *des Products*

$$1. \quad \mathrm{P} = \mathrm{a.b.c.d \ldots m.n}$$

aufeinander folgen, kann nach Belieben verändert werden, ohne dafs sich der Werth des Products änderte.

II. *Die Anzahl* $\overset{\nu}{\mathrm{x}}$ *der verschiedenen möglichen Arten, in welchen die Factoren auf einander folgen können, ist*

$$2. \quad \overset{\nu}{\mathrm{x}} = 1.2.3.4.5 \ldots \nu.$$

Beispiel. Alle die

$$3. \quad 1.2.3.4 = 24$$

Producte

$$4. \quad \begin{cases} 2.3.7.9, & 2.7.3.9, & 3.2.7.9, & 3.7.2.9, & 7.2.3.9, & 7.3.2.9, \\ 2.3.9.7, & 2.9.3.7, & 3.2.9.7, & 3.9.2.7, & 9.2.3.7, & 9.3.2.7, \\ 2.9.7.3, & 2.7.9.3, & 9.2.7.3, & 9.7.2.3, & 7.2.9.3, & 7.9.2.3, \\ 9.3.7.2, & 9.7.3.2, & 3.9.7.2, & 3.7.9.2, & 7.9.3.2, & 7.3.9.2 \end{cases}$$

haben sämmtlich denselben Werth 378.

Erster Beweis. *A.* Nach dem Lehrsatze (§. 4.) können die Multiplicationszeichen wo man will *weggelassen* werden, ohne dafs der Werth des Products sich änderte.

Man lasse sie in (1.) *alle bis auf irgend eins*, z. B. bis auf das zwischen g und h, weg, so ist

$$5.\quad P = abcd\ldots.g \times hi\ldots.lmn.$$

Dieser Ausdruck von P heifst: es soll die *Zahl* $abcd\ldots.g$, die durch G bezeichnet werden mag, mit der Zahl $hi\ldots.lmn$, welche H sein mag, multiplicirt werden: das Product davon sei P. Es ist also

$$6.\quad P = G.H.$$

B. Die Zahl

$$7.\quad H = hi\ldots.lmn \quad (A.)$$

ist aber (nach §. 1.) nichts anders als

$$8.\quad H = hi\ldots.lm.n:$$

daher ist, wenn man der Kürze wegen die Zahl $hi\ldots.lm$ durch M bezeichnet,

$$9.\quad H = M.n.$$

C. Nun schreibe man so viele *Einheiten* in eine horizontale Reihe, als deren die Zahl M enthält, und so viele solcher *Reihen* unter einander, als *Einheiten* in der Zahl n enthalten sind, nemlich wie folgt:

$$10.\quad \left.\left\{\begin{array}{cccccccc} \multicolumn{8}{c}{\overbrace{\hphantom{1\ 1\ 1\ 1\ \ldots.\ 1}}^{M}} \\ 1 & 1 & 1 & 1 & . & . & . & . \; 1 \\ 1 & 1 & 1 & 1 & . & . & . & . \; 1 \\ 1 & 1 & 1 & 1 & . & . & . & . \; 1 \\ . & . & . & . & . & . & . & . \; . \\ 1 & 1 & 1 & 1 & . & . & . & . \; 1 \end{array}\right\}\right. n.$$

Hier sind offenbar in Allem so viele Einheiten hingeschrieben worden, als das Product $M.n$ und folglich die Zahl H enthält, und man findet ihre Anzahl, wenn man M, wie es sein soll, mit n multiplicirt. Man findet aber auch ihre Anzahl, wenn man n mit M multiplicirt; denn es befinden sich in jeder *verticalen* Reihe n Einheiten (nemlich so viele als horizontale *Reihen*), und solcher *verticalen* Reihen sind M vorhanden (nemlich so viele als *Einheiten* in jeder horizontalen Reihe). Also ist

$$11.\quad M.n = n.M,$$

das heifst, es ist

$$12.\quad hi\ldots.lm \times n = n \times hi\ldots.lm = H \quad (8.).$$

D. Aber zufolge (§. 4.) ist auch, da das Multiplicationszeichen zwischen n und h weggelassen werden kann,

$$13.\quad n \times hi \ldots. lm = nhi \ldots. lm,$$

also ist auch zufolge (12. und 7.)

$$14.\quad nhi \ldots. lm = hi \ldots. lmn = H,$$

und folglich, vermöge (6.),

$$15.\quad P = G.nhi \ldots. lm = abcd \ldots. g \times nhi \ldots. lm \text{ (5.)},$$

mithin nach (§. 4.) auch

$$16.\quad P = abcd \ldots. gnhi \ldots. lm,$$

und da vermöge (§. 4.) auch

$$17.\quad P = abcd \ldots. ghi \ldots. lmn$$

ist,

$$18.\quad abcd \ldots. gnhi \ldots. lm = abcd \ldots. ghi \ldots. lmn = P,$$

oder auch, da zufolge (§. 4.) $abcd \ldots. gnhi \ldots. lm$ dasselbe ist, wie $a.b.c.d \ldots$ $\ldots g.n.h.i \ldots. l.m$,

$$19.\quad a.b.c.d \ldots. g.n.h.i \ldots. l.m = a.b.c.d \ldots. g.h.i \ldots. l.m.n = P.$$

E. Hieraus folgt, dafs der *letzte* Factor n von P *jede beliebige* Stelle einnehmen kann, ohne dafs der Werth von P sich änderte; denn, eben so wie er hier zwischen g und h getreten ist, kann er auch zwischen zwei *beliebige* andere Factoren treten, und selbst vor *alle* ihm vorhergehende Factoren; denn für den letzten Fall darf man sich P nur als $1.a.b.c.d \ldots. l.m.n$ vorstellen und n zwischen 1 und den Factor a treten lassen.

F. Nun setze man für den Augenblick *voraus*, in einem Product von $\nu-1$ Factoren, z. B. in dem Product

$$20.\quad X_1 = a.b.c.d \ldots. l.m,$$

welches also hier

$$21.\quad P = X_1.n = a.b.c.d \ldots. l.m.n$$

giebt, dürfen wirklich *alle* Factoren nach Belieben vertauscht werden, ohne dafs der Werth von X_1 sich änderte, so ändert sich offenbar durch alle diese Vertauschungen auch der Werth von $P = X_1 n$ nicht.

G. Wie oben gezeigt, kann aber der *letzte* Factor n in P (21.) irgendwo anders hin, also *vor m* treten, ohne dafs dadurch *der Werth von P* sich änderte. Also kann P auch durch

$$22.\quad P = X_2.m$$

ausgedrückt werden, wo X_2, eben wie X_1, $\nu-1$ Factoren enthält, und zwar *alle* Factoren von P bis auf den *einen* m.

H. Ist nun die Voraussetzung richtig, dafs in einem Product von $\nu-1$ Factoren alle diese Factoren nach Belieben vertauscht werden können, ohne dafs der Werth des Products sich änderte, so können alle diese möglichen Vertauschungen auch in X_2 geschehen, ohne dafs der Werth von X_2 und mithin zufolge (22.) der Werth von P ein anderer würde.

I. Unter den verschiedenen *möglichen* Formen von X_2 werden nothwendig auch solche sein, die l zum *letzten* Factor haben. *Vor* diesen letzten Factor kann, in irgend einer derselben, wieder dem oben Bewiesenen zufolge, in (22.) m treten, ohne dafs P sich änderte: also kann auch P durch

$$23. \quad P = X_3 . l$$

ausgedrückt werden, wo X_3, eben wie X_2 und X_1, $\nu-1$ Factoren enthält; und zwar *alle* Factoren von P bis auf den *einen* l.

K. Hier können abermals, immer insofern die obige Voraussetzung (*F.*) richtig ist, die Factoren in X_3 auf alle mögliche Arten vertauscht werden, ohne dafs der Werth von X_3, und folglich auch ohne dafs P sich ändert.

L. Nimmt man aus den verschiedenen Formen von X_3 eine, in welcher k der *letzte* Factor ist, so kann in (23.) vor k wieder l treten und folglich P auch durch $X_4 . k$ ausgedrückt werden. Und so weiter.

M. Alle die verschiedenen Ausdrücke

$$24. \quad X_1 . n, \quad X_2 . m, \quad X_3 . l, \quad X_4 . k, \; \ldots . \; X_\nu a$$

geben also sämmtlich den *gleichen* Werth von P, stets insofern die Voraussetzung richtig ist, dafs in einem Product von $\nu-1$ Factoren die sämmtlichen Factoren nach Belieben vertauscht werden dürfen.

N. Die verschiedenen Ausdrücke (24.) von P enthalten aber, wie aus dem ersten Beweise des Lehrsatzes (§. 5.) hervorgeht, *alle möglichen* Vertauschungen der *sämmtlichen ν Factoren von P*. Also folgt bis hieher, dafs, *insofern* es wahr ist, dafs in einem Product von $\nu-1$ Factoren die Factoren auf *alle mögliche* Arten vertauscht werden dürfen, ohne dafs der Werth des Products sich änderte, das *Gleiche* auch für ein Product von ν Factoren gilt.

O. In einem Product von zwei Factoren, z. B. a und b, dürfen aber wirklich die beiden Factoren auf die für sie *möglichen zwei* Arten vertauscht werden, ohne dafs der Werth des Productes sich ändert. Dieses folgt aus (*C.*): denn so wie dort $M.n = n.M$ ist (11.), so ist auch $a.b = b.a$.

Also folgt aus (*N.*), dafs auch in einem Product von 3 Factoren die

Factoren auf alle mögliche Arten vertauscht werden dürfen, und folglich auch in Producten von 4. 5. 6 u. s. w. Factoren; was zu beweisen war.

P. Die Zahl der möglichen Vertauschungen von ν Factoren ist, wie unmittelbar aus dem Lehrsatz (5.) hervorgeht, $x_\nu = 1.2.3.4 \ldots \nu$; wie es (2.) ausdrückt.

Anm. Die Hauptpuncte dieses Beweises sind, dafs erstlich der *letzte* Factor eines Products seine Stelle mit jedem vorhergehenden vertauschen kann; sodann, dafs, insofern die $\nu-1$ Factoren eines Products nach Belieben vertauscht werden dürfen, jeder der ν Factoren zum *letzten* gemacht werden kann, dafs auf solche Weise *alle möglichen* Vertauschungen von ν Factoren erlangt werden, und dann, dafs die vorausgesetzte Zulässlichkeit der Vertauschung der Factoren für *zwei* Factoren *wirklich* stattfindet. Der Beweis stützt sich auf die Lehrsätze (§. 4. u. 5.).

Zweiter Beweis. Q. Man setze, wie oben in (F.), einen Augenblick voraus, es dürfen in dem Product von $\nu-1$ Factoren

$$25. \quad X_1 = abcd \ldots lm$$

die Factoren auf alle möglichen Arten vertauscht werden, ohne dafs der Werth des Products sich ändere. Ist diese Voraussetzung richtig, so wird der Werth des Products

$$26. \quad P = X_1.n = abcd \ldots lm.n$$

von ν Factoren sich nicht ändern, wie man auch in X_1 die $\nu-1$ Factoren $a, b, c, d \ldots m$ versetzen mag.

R. Nun ist P (26.) nach (§. 1.) nichts anderes als

$$27. \quad P = L.m.n$$

wenn man das Product $abcd \ldots l$ durch L bezeichnet; das heifst, es mufs L erst m mal und das was herauskommt n mal genommen werden.

S. Auf dieselbe Weise, wie in (B. §. 4.), folgt aber, dafs $L.m.n$ nichts anders als $L.mn$, also auch

$$28. \quad P = L.mn$$

ist, das heifst, dafs man P auch findet, wenn man L *sogleich* mit der Zahl mn multiplicirt, die das Product von m und n ist.

T. Ferner folgt auf dieselbe Weise wie oben in (C.), dafs $mn = nm$ ist. Mithin ist auch

$$29. \quad P = L.nm.$$

Und da nach (§. 4. B.) auch $L.n.m = L.nm$ ist, so folgt, dafs auch

$$30. \quad P = L.n.m.$$

das heifst

$$31. \quad P = abcd \ldots . l.n.m$$

oder auch nach (§. 1.)

$$32. \quad P = abcd \ldots . ln.m$$

ist, was der Kürze wegen durch

$$33. \quad P = X_2.m$$

bezeichnet werden mag.

Von hier ab weiter ist der Beweis im Wesentlichen derselbe wie der Theil (*H.* bis *P.*) des ersten Beweises.

Anm. Dieser zweite Beweis bedarf nicht des vollständigen Lehrsatzes (§. 4.). Er nimmt daraus nur was ihm nöthig ist, nemlich den Theil (*B.*). Der vollständige Satz (§. 4.) kann indessen in andern Fällen Anwendung finden.

Dritter Beweis. *U.* Das Product

$$34. \quad P_\nu = (1+a)(1+b)(1+c)(1+d) \ldots . (1+n)$$

enthält, wenn man die angedeuteten Multiplicationen ausführt, zufolge (§. 2.) nächst der Einheit *alle möglichen* Producte von a, b, c, d, ... n zu einem, zwei, drei, vier u. s. w. bis ν Factoren. Zum Beispiel

$$35. \quad (1+a)(1+b)(1+c)(1+d) = \begin{array}{l} 1 \\ +a+b+c+d \\ +ab+ac+ad+bc+bd+cd \\ +abc+abd+acd+bcd \\ +abcd. \end{array}$$

V. Man *setze einen Augenblick voraus,* dafs in einem Product von ν Factoren a, b, c, d, ... n, also auch von *weniger* als ν Factoren, die Factoren nach Belieben vertauscht werden können, ohne dafs der *Werth* des Products sich änderte.

W. Nun vertausche man z. B. in (35.) *rechterhand* die Factoren a, b, c, d der einzelnen Glieder nach Belieben wirklich, so werden dadurch weder *mehr* Glieder, noch Glieder entstehen können, die *andere* Factoren enthielten als die vorigen; denn es sind von jeder *Art* von Gliedern, zu einem, zwei, drei und vier Factoren, wie §. 2. *beweiset,* immer *alle möglichen* vorhanden. Die Glieder, welche man durch die Vertauschung erhält, werden von den vorigen in sich durch nichts weiter als durch die verschiedene Aufeinanderfolge ihrer Factoren verschieden sein. Dadurch ändert sich aber *nach der Voraussetzung* ihr Werth nicht, also auch nicht die Summe der Glie-

der, und folglich auch der Werth z. B. von $(1+a)(1+b)(1+c)(1+d)$ in (35.) nicht.

Die Vertauschung von a, b, c und d in (35.) bringt aber *linkerhand* nichts anderes hervor, als die Vertauschung der Factoren $1+a$, $1+b$, $1+c$, $1+d$ *selbst;* also folgt bis hierher, dafs, wenn die Voraussetzung: es ändere sich der Werth eines Productes von ν und weniger Factoren (hier in dem Beispiel von 4 Factoren) durch die Vertauschung der Factoren nicht, *für die Werthe* a, b, c, d, ... der Factoren richtig ist, dasselbe auch für die *um 1 gröfseren Werthe* $1+a$, $1+b$, $1+c$, $1+d$, ... der Factoren gilt.

X. Daraus folgt weiter, dafs die Voraussetzung für die Werthe a, b, c, d, ... der Factoren gilt, wenn sie für die um 1 *kleineren* Werthe $a-1$, $b-1$, $c-1$, $d-1$, ... derselben stattfindet, also ferner, auch schon, wenn sie für die Werthe $a-2$, $b-2$, $c-2$, $d-2$, ... gilt, und so weiter: also auch dann schon, wenn sie, im Fall etwa a der *kleinste* der Factoren ist, für die Werthe 1, $b-(a-1)$, $c-(a-1)$, $d-(a-1)$, ..., mithin *blofs für* $\nu-1$ *Factoren* gilt; denn 1 hat als Factor keine Wirkung.

Y. Der *vorausgesetzte* Satz, dafs die Factoren eines Products nach Belieben vertauscht werden können, gilt also für ν beliebige Factoren schon dann, wenn er für $\nu-1$ beliebige Factoren gilt. Daraus folgt, dafs er für $\nu-1$ Factoren, also auch für ν Factoren gilt, wenn er für $\nu-2$ Factoren stattfindet u. s. w.: zuletzt also blofs, wenn z. B. $1.a = a.1$ ist. Dies aber ist offenbar der Fall: also gilt der Satz, dafs sich der Werth eines Products beliebiger Factoren durch die Versetzung derselben nicht ändert, wirklich; was zu beweisen war.

Anm. Dieser Beweis stützt sich *blofs* auf den Lehrsatz (§. 2.).

Anm. zu §. 2. bis 6. Man wolle an die scheinbar zu viele Allgemeinheit und Abstraction, so wie an die scheinbar zu grofse Zurüstung für so einfache Dinge wie die vorhergehenden, von welchen sich schon durch blofse Anschauung eine Überzeugung (freilich dann nur eine Art von Überzeugung) erlangen läfst, nicht Anstofs nehmen. Die Übung des Lernenden im Denken, Schliefsen und Urtheilen, also auch in der Abstraction, ist einer der *Zwecke* der gegenwärtigen Schrift. Die Zurüstung für den gegenwärtigen Hauptsatz §. 6., in den vorhergehenden, dürfte, wenn man vollkommene *Strenge* verlangt, nöthig sein. Die Beweise No. 1. und 2. §. 6. dürften sich nicht wohl kürzer und nicht ohne die vorhergehenden Sätze mit *gleicher Strenge* geben lassen.

§. 7.

Lehrsatz.

Die **Vorzeichen** $+$ *und* $-$ *von* ν *Factoren* a, b, c, d, ... n *eines Products*

$$1.\quad P = abcd \ldots n$$

können auf

$$2.\quad 2^{\nu-1}$$

Arten verändert werden, ohne dafs das **Vorzeichen** *des Products sich änderte.*

Beispiel. Für $\nu = 4$ ist

$$3.\quad +P$$

$$= +a.+b.+c.+d = +a.+b.-c.-d = +a.-b.+c.-d = -a.+b.+c.-d$$
$$= +a.-b.-c.+d = -a.+b.-c.+d = -a.-b.+c.+d = -a.-b.-c.-d$$

und

$$4.\quad -P$$

$$= +a.+b.+c.-d = +a.+b.-c.+d = +a.-b.+c.+d = -a.+b.+c.+d$$
$$= +a.-b.-c.-d = -a.+b.-c.-d = -a.-b.+c.-d = -a.-b.-c.+d;$$

und mehr als diese $2^{\nu-1} = 2^3 = 8$ Veränderungen der Zeichen sind für $+P$, so wie für $-P$, nicht möglich.

Beweis. *A.* Es sei für $\varkappa < \nu$ Factoren $a, b, c, d, \ldots k$

$$5.\quad a.b.c.d \ldots k = K,$$

und für die $\varkappa+1$ Factoren $a, b, c, d, \ldots k, l,$

$$6.\quad a.b.c.d \ldots k.l = l.K = L.$$

B. In dem Product der zwei Factoren l und K, nemlich in

$$7.\quad l.K = L$$

können offenbar die Vorzeichen von l und K nur auf *2 verschiedene* Arten verändert werden, ohne dafs das Vorzeichen von L sich änderte. Nemlich es ist nur

$$8.\quad +L = +K.+l = -K.-l \quad \text{und}$$
$$9.\quad -L = +K.-l = -K.+l.$$

C. Nun setze man, in dem Product K von $\varkappa$ Factoren können die Vorzeichen der Factoren $x_\varkappa$ *mal* verändert werden, ohne dafs das Vorzeichen von K sich änderte. Alsdann folgt aus (8. u. 9.), dafs in dem Product L von $\varkappa+1$ Factoren die Vorzeichen der Factoren $2x_\varkappa$ *mal* verändert werden können, ohne dafs das Vorzeichen von L sich änderte. Dieses gilt für *jeden* Werth von $\varkappa$, von 2 an, so weit man will.

D. Es können aber, wie ebenfalls aus (8. u. 9.) folgt, wenn man sich unter K nur einen einfachen Factor vorstellt, für $z=2$ Factoren die Vorzeichen der Factoren auf 2 verschiedene Arten verändert werden, ohne dafs das Vorzeichen des Products sich änderte; also ist solches für $z=3$ Factoren auf $2.2=2^2$, für $z=4$ Factoren auf $2.2^2=2^3$, für $z=5$ Factoren auf $2.2^3=2^4$ u. s. w. und allgemein für $z=\nu$ Factoren auf $2^{\nu-1}$ Arten möglich; wie es der Lehrsatz behauptet.

§. 8.

Erklärungen.

I. Insbesondere bei *ganzen* Zahlen kann man im Allgemeinen diejenige Zahl ***Rest*** nennen, welche entsteht, wenn mit irgend einer Zahl z ein Vielfaches, z. B. das $q$fache einer andern Zahl u durch das Minuszeichen verbunden wird. Desgleichen kann im Allgemeinen jene ***Anzahl*** des Vielfachen von u ***Quotient*** heifsen, die Zahl z ***Dividend***, und die Zahl u ***Divisor***, so dafs in der Gleichung

$$1. \quad z-qu=r \quad \text{oder} \quad z=qu+r$$

z der ***Dividend***, u der ***Divisor***, q der ***Quotient*** und r der ***Rest*** ist.

Der ***Quotient*** q ist allgemein ***ganz willkürlich***, und kann z. B. jede beliebige ***positive ganze*** Zahl sein, also $=0, 1, 2, 3, 4, \ldots,$ bis ins Unendliche. Er könnte selbst jede beliebige ***negative ganze*** Zahl sein; allein dann pflegt man r nicht mehr ***Rest***, sondern ***Summe*** zu nennen.

II. Zu ***jedem*** beliebigen Werth von q gehört vermöge der Gleichung (1.) natürlich ***ein***, und ***nur ein*** Werth von r; also zu jedem ***andern*** Werth von q ein anderer Werth von r, und es giebt folglich eben so viele Werthe von r, als von q; mithin ***unzählige***. Zu jedem Werth von r gehört umgekehrt ein Werth von q, und ***nur einer***. Die Werthe von r können ***positiv***, ***null*** und ***negativ*** sein. Sie sind ***positiv*** so lange $qu<z$, ***negativ*** wenn $qu>z$, und null wenn $qu=z$ ist. Letzteres ist der Fall, wenn u in z ***aufgeht***; und ***nur dann***.

III. *a.* Die Anzahl der ***positiven*** r ist für positive z, q und u immer ***begrenzt***. Es giebt ihrer so viele als Werthe von q, für welche qu nicht gröfser als z ist. Wenigstens ***einen*** positiven Werth von r aber giebt es auch für positive q ***immer***, selbst wenn $z<u$ ist; in welchem Fall er zu $q=0$ gehört und z selbst ist. Ist $z>u$, so kann es der positiven Werthe von r, die kleiner als u sind, mehrere geben.

b. Die Anzahl der *negativen* Werthe von r ist immer *unendlich grofs.* Alle r sind negativ, die zu positiven Werthen von q gehören, für welche $qu > z$ ist; und solcher Werthe von q giebt es unzählige, da q ohne Ende wachsen kann.

c. Der Werth 0 von r kommt für *ganzzahlige* q, wie schon bemerkt, nur dann vor, wenn u in z *aufgeht.* Verlangt man aber den Werth 0 von r auch in dem Fall, wenn u in z *nicht aufgeht,* so bekommt der Quotient $q = \frac{z}{u}$ keine *ganze* Zahl zum Werthe. Er ist alsdann ein *Bruch.* Geht u in z auf, so kann man den Quotienten zur Unterscheidung *ganzzahlig* nennen. Der *Bruch* $\frac{z}{u}$ heifst *unecht,* wenn $z > u$, *echt,* wenn $z < u$ ist.

IV. Da die Werthe, welche der Rest r haben kann, alle von einander verschieden sind, nemlich jeder von dem nächsten um u, so wie q um 1 wächst oder abnimmt, so wird es nothwendig immer, sowohl unter den positiven als unter den negativen Werthen von r, *einen* und *nur einen* geben, der, abgesehen vom Zeichen, durch eine *kleinere Zahl* ausgedrückt ist, als alle übrigen *seiner Art.*

Da nun in Dem, was weiter folgt, die beiden Reste r, die unter allen übrigen ihrer Art die *kleinsten* Zahlenwerthe haben, *insbesondere* in Betracht kommen, so wird es gut sein, ihnen, nebst den ihnen correspondirenden Quotienten für *ganze* Zahlen, eine ausschliefsliche abgekürzte *Benennung* zu geben.

a. Es sollen die beiden Reste, welche die *kleinsten* Zahlenwerthe haben, *echte* Reste heifsen; und zwar derjenige mit dem Pluszeichen *positiver echter Rest,* der mit dem Minuszeichen *negativer echter Rest.* Derjenige von beiden, welcher, falls die beiden Reste ungleich sind, abgesehen vom Zeichen, den *kleinsten* Zahlenwerth hat, und der also dann von *allen möglichen* Resten den kleinsten Zahlenwerth hat, soll *zeichenfrei-* oder *unbedingt echter Rest,* oder auch blofs *kleinster Rest* heifsen; gleichviel ob er positiv oder negativ sei.

b. Die zu den beiden echten Resten gehörigen *Quotienten* sollen, um sie von dem Quotienten $\frac{z}{u}$ selbst, den man, er mag eine ganze Zahl oder ein Bruch sein, *genauen Quotienten* nennen kann, zu unterscheiden, *nächste Quotienten* heifsen; und zwar soll der zu dem *positiven* echten Rest gehörige Quotient *unternächster Quotient,* der zu dem *negativen* echten Rest gehörige Quotient *übernächster Quotient* genannt werden. Derjenige

von diesen beiden Quotienten, welcher dem *unbedingt nächsten* oder *kleinsten* Rest angehört, soll *unbedingt nächster Quotient* heifsen. Die Ursach der Wahl dieser Benennungen wird sich im folgenden Paragraphen zeigen.

Um die *nächsten* Quotienten, mit Anzeige des Dividenden und Divisors, von dem *genauen* Quotienten zu unterscheiden, welchem die gewöhnliche Bezeichnung $z:u$ oder $\frac{z}{u}$ vorbehalten bleibt, soll der *unternächste Quotient* durch $(z+:u)$, der *übernächste Quotient* durch $(z-:u)$ und der *unbedingt nächste* Quotient durch $[z:u]$ bezeichnet werden.

Beispiele. *No. 1.* Der Dividend z sei $=33$, der Divisor $u=11$, so giebt die Gleichung (1.)

$$2.\quad 33=0.11+33=1.11+22=2.11+11=3.11+0=4.11-11$$
$$=5.11-22\ldots.$$

Hier sind der *positive*, der *negative* und der *unbedingt nächste Rest* alle drei Null. Der *übernächste*, der *unternächste* und der *unbedingt nächste* Quotient sind alle drei $=3$. Der *genaue* Quotient ist gleichfalls $=3$, also *ganzzahlig;* folglich ist hier $(z+:u)=(z-:u)=[z:u]=z:u=\frac{z}{u}$.

No. 2. Der Dividend z sei wieder $=33$, aber der Divisor $u=7$, so ist

$$3.\quad 33=0.7+33=1.7+26=2.7+19=3.7+12=4.7+5=5.7-2$$
$$=6.7-9=7.7-16\ \ldots.$$

Hier ist der *positive echte* Rest $=+5$, der *negative echte* Rest $=-2$, der *unbedingt echte* Rest $=-2$. Der *unternächste Quotient* $(z+:u)$ ist $=4$, der *übernächste Quotient* $(z-:u)=5$, der *unbedingt nächste Quotient* $[z:u]=5$, der *genaue Quotient* $z:u$ oder $\frac{z}{u}=\frac{33}{7}$, also ein *Bruch,* und zwar ein *unechter* Bruch.

No. 3. Der Dividend z sei abermals $=33$, der Divisor $u=41$, so ist

$$4.\quad 33=0.41+33=1.41-8=2.41-49=3.41-90\ \ldots.$$

Hier ist der *positive echte Rest* $=+33$, der *negative echte* Rest $=-8$, der *unbedingt echte* Rest $=-8$. Der *unternächste Quotient* $(z+:u)$ ist $=0$, der *übernächste Quotient* $(z-:u)=1$, der *unbedingt nächste* Quotient $[z:u]=1$. Der genaue Quotient $z:u$ oder $\frac{z}{u}$ ist $=\frac{33}{41}$, also ein *Bruch,* und zwar ein *echter* Bruch.

§. 9.

Erläuterungen zum vorigen Paragraphen.

I. Wenn der Divisor u in den Dividenden z *aufgeht*, so ist immer

$$1. \quad (z+:u) = (z-:u) = [z:u] = z:u = \frac{z}{u}.$$

Der *negative*, der *positive* und der *unbedingt echte Rest* sind alle drei Null, und der *unternächste*, der *übernächste* und der *genaue* Quotient sind einander *gleich* und *ganze* Zahlen. Dieses ist an sich klar, und das Beispiel (No. 1. §. 8.) macht es anschaulich.

II. Wenn der Divisor u in den Dividenden z nicht *aufgeht*, so sind die *absoluten Zahlenwerthe* oder, wie man füglich auf deutsch sie nennen kann, die *zeichenfreien Zahlenwerthe* beider echten Reste nothwendig unter den Zahlen

$$2. \quad 1, 2, 3, 4, \ldots \; u-1$$

anzutreffen. Denn wenn man, der Gleichung

$$3. \quad z - qu = r \quad (§. 8. \; 1.)$$

gemäfs, u von z so oft *als möglich* abzieht, so kann das r, welches bleibt, nicht mehr *gröfser* als u sein; auch, in dem Fall, wenn z mit u *nicht* aufgeht, weder u noch 0. Also kann der *positive echte* Rest nur eine der Zahlen (2.) sein. Zieht man u noch weiter ab, so kann der nächste Rest, welches der negative echte Rest ist, weder $< -u$, noch 0, noch $-u$ sein, also wiederum nur eine der Zahlen (2.), mit dem Minuszeichen.

Ganz eben so verhält es sich, wenn z und u beide *negativ* sind, denn dann heifst die Gleichung (3.)

$$4. \quad \begin{cases} -z + qu = -r \text{ oder} \\ -(z - qu) = -r. \end{cases}$$

Auch in diesem Fall sind die absoluten Zahlenwerthe beider echten Reste nothwendig unter den Zahlen (2.) anzutreffen.

III. Der *algebraische* Werth des *positiven echten* Restes ist immer um den *Divisor* gröfser, als der *algebraische* Werth des *negativen echten* Restes; und von den *zeichenfreien* Zahlenwerthen der beiden Reste ist die *Summe* immer dem Divisor gleich.

Denn den *negativen echten* Rest, welcher durch $-\varrho$ bezeichnet werden mag, erhält man aus dem *positiven echten* Rest, welcher $+r$ sein mag, wenn man den Divisor u von $+r$ noch einmal abzieht, so dafs also $+r-u = -\varrho$ ist: mithin ist $+r$ um u gröfser als $-\varrho$. Ferner folgt aus $+r-u$

$= -\varrho$, $+r+\varrho = +u$, und folglich ist die Summe der *zeichenfreien* Zahlenwerthe r und ϱ der beiden Reste dem Divisor u gleich.

IV. Der Zahlenwerth des *unbedingt echten* Restes kann nicht gröfser als *die Hälfte des Divisors* sein.

Denn da die absoluten Zahlenwerthe r und ϱ der beiden echten Reste zufolge (III.) u ausmachen, so können nicht beide zugleich gröfser als $\frac{1}{2}u$ sein; sonst wäre $+r+\varrho > u$, nicht $= u$. Also können r und ϱ nur entweder beide $= \frac{1}{2}u$ sein, oder derjenige, welcher von beiden der kleinere und welcher dann der *unbedingt echte Rest* ist, mufs $< \frac{1}{2}u$ sein. In *keinem* Falle also ist der *unbedingt echte* Rest *gröfser* als $\frac{1}{2}u$.

Auch verhält es sich ganz so, wenn z und u beide *negativ* sind.

V. Die *zeichenfreien Zahlenwerthe* r und ϱ des positiven und des negativen echten Restes können nur dann *einander gleich* sein, wenn der Divisor u durch 2 theilbar ist; jedoch sind sie es dann nicht nothwendig. Sie sind aber nothwendig *einander nicht gleich*, wenn der Divisor u nicht mit 2 aufgeht, was auch der Dividend z sein mag.

Denn da immer $r+\varrho = u$ ist, so ist für $r = \varrho$, $u = 2r = 2\varrho$: also mufs, wenn $r = \varrho$ sein soll, u nothwendig mit 2 aufgehen. Jedoch kann u mit 2 aufgehen, ohne dafs $r = \varrho$ ist; denn in $r+\varrho = u$ kann r mit 2 dividirt den Rest 1 lassen, und ϱ ebenfalls, $r+\varrho$ also den Rest 2, und also kann $r+\varrho = u$ sein, ohne dafs $r = \varrho$ wäre. Ferner kann nicht $r = \varrho$ sein, wenn u *nicht* mit 2 aufgeht; denn $r+\varrho = u$ giebt für $r = \varrho$, $u = 2r = 2\varrho$, welches immer mit 2 aufgeht.

VI. Der *unternächste Quotient*, zu dem *positiven* echten Rest gehörig, ist immer um einen *echten* Bruch oder um weniger denn 1 *kleiner;* und der *übernächste Quotient*, zu dem negativen echten Rest gehörig, ist immer um einen *echten* Bruch oder um weniger als 1 *gröfser*, als der *genaue* Quotient; so dafs es also keine *ganze* Zahlen giebt, die dem *genauen* Quotienten *näher kämen*, als die jener beiden Quotienten. Dieser Umstand ist daraus klar, dafs man von dem positiven unmittelbar zu dem negativen echten Rest gelangt, wenn man den Divisor von ersterem noch *einmal* abzieht, während der genaue Quotient *zwischen* dem unternächsten und dem übernächsten Quotienten liegt. Dieser Umstand ist der *Grund*, weshalb wir die beiden Quotienten *nächste* nannten, und zwar den zu dem echten *positiven* Rest gehörigen Quotienten *unternächsten*, den zu dem echten *negativen* Rest gehörigen Quotienten *übernächsten* Quotienten, indem ersterer immer *kleiner*, letzterer immer *gröfser* ist, als der *genaue* Quotient.

VII. Der *übernächste* Quotient ist immer um 1 gröfser, als der *unternächste.*

VIII. Kein **Bruch**, z. B. $\frac{z}{u}$, kann einer *ganzen* Zahl gleich sein.

Denn $\frac{z}{u}$ ist dann ein **Bruch**, wenn man durch wiederholtes Abziehen des Divisors u von z *nicht* auf den Rest 0 kommt (§. 8. III. *c.*), sondern auf einen positiven echten Rest r, der > 0 und $< u$ ist. Also ist dann in der Gleichung

$$4. \quad z = qu + r$$

$r > 0$ und $< u$. Dividirt man diese Gleichung mit u, so folgt, dafs der *genaue* Quotient

$$5. \quad \frac{z}{u} = q + \frac{r}{u},$$

das heifst gleich der Summe einer *ganzen* Zahl q und des Bruchs $\frac{r}{u}$ ist, der > 0 und < 1 ist. Er ist also weder die ganze Zahl q, noch die ganze Zahl $q+1$, noch weniger eine andere ganze Zahl, also überhaupt *keine* ganze Zahl.

§. 10.

Erklärungen und Erläuterungen.

I. In der Gleichung

$$1. \quad z = qu + r,$$

in welcher z der *Dividend*, u der *Divisor*, q der *Quotient*, r der **Rest** und q *willkürlich* ist, wenn z und u gegeben sind, kommt es, wenn z und u *ganze* Zahlen sind, um für r ebenfalls eine *ganze* Zahl zu haben, wie schon oben bemerkt, nicht darauf an, dafs q eine ganze *positive* Zahl sei: es kann q auch jede beliebige *negative* ganze Zahl sein. r ist *immer* eine ganze Zahl, welche positive oder negative ganze Zahl auch q sein mag: denn aus (1.) folgt $r = z - qu$, und wenn z, q und u ganze Zahlen sind, so ist auch $z - qu$ eine ganze Zahl, und also auch r, da ein **Bruch** nie einer ganzen Zahl gleich sein kann (§. 9. VIII.).

II. Die Zerlegung einer ganzen Zahl z in irgend ein Vielfaches qu einer andern ganzen Zahl u und in einen Rest r, nach (1.), so dafs man z als die *algebraische* Summe jenes Vielfachen und des Restes betrachtet, findet in der gesammten Theorie der Zahlen unzählige Anwendungen. Diese Zerlegung ist sogar eines der *Hauptmittel*, durch welches diese Theorie zu vielen, selbst fast zu den meisten ihrer Sätze gelangt; denn sie findet solche

häufig durch die Untersuchung Dessen, was bei dieser oder jener Verbindung von Zahlen z, die *Reste* derselben r in Beziehung auf andere Zahlen u geben. Schon z. B. die Theilbarkeit oder Nicht-Theilbarkeit einer Zahl z durch u hangt blofs davon ab, ob unter den verschiedenen Werthen, welche der Rest r haben kann, auch der Werth Null ist, oder nicht.

III. Es kommt nun aber bei sehr vielen Untersuchungen, die Eigenschaften der Zahlen betreffend, auf die *Gröfse* des Quotienten q ganz und gar nicht an, sondern nur auf die *Gröfse des Restes* r allein, und rücksichtlich des *Quotienten* einzig und allein *darauf*, dafs er eine *ganze* Zahl sei. Zum Beispiel wenn z_1, z_2, z_3, ... z_x mehrere verschiedene ganze Zahlen wären, von welchen irgend eine *Verbindung* in Beziehung auf eine andere ganze Zahl u untersucht werden soll, und es wäre etwa

$$2.\quad \begin{cases} z_1 = q_1 u + r_1, \\ z_2 = q_2 u + r_2, \\ z_3 = q_3 u + r_3, \\ \dots\dots\dots \\ z_x = q_x u + r_x, \end{cases}$$

so kann es sein, dafs sich diese Untersuchung schon durch diejenige der *gleichen* Verbindung der *Reste* r, etwa der positiven oder negativen *echten* Reste, oder auch der *unbedingt echten* Reste, *allein* ausführen läfst und dafs dabei die *Gröfse* der Quotienten q *ganz gleichgültig* ist. Es ist dies immer der Fall, wenn die *Resultate dieselben* bleiben, *welche* ganzzahligen Werthe auch die Quotienten q haben mögen: was, wie sich in der Folge zeigen wird, sehr häufig vorkommt. Wo es so ist, entsteht dann offenbar schon der Gewinn, dafs man es statt mit den Zahlen z, die *sehr grofs* sein können, nur mit den Resten r, die, wenn man die *echten* Reste nimmt, immer *kleiner als* u sind, also vielleicht nur noch mit *viel* kleineren Zahlen zu thun hat: was indessen häufig noch der geringste Gewinn ist.

IV. Es kann also, wie gesagt, sein, dafs es auf die *Gröfse* z. B. ganzzahliger Quotienten q bei dem Ausdruck von Zahlen z, als Summen von Vielfachen einer andern Zahl u und eines Restes, so wie auch zu noch anderen Zwecken, auf die *Gröfse* dieser oder jener ganzen Zahlen überhaupt *gar nicht* ankommt, sondern nur allein darauf, dafs angezeigt werde, die Quotienten, oder sonst jene Zahlen, *seien ganze Zahlen*.

In solchen Fällen würde es offenbar unnütz sein, die verschiedenen Quotienten oder Zahlen durch *verschiedene* Buchstaben oder Zeichen zu unter-

scheiden. Es geschieht schon Alles, was nöthig ist, wenn man irgend ein *ausschliefsliches* Zeichen blofs *für den Begriff der ganzen Zahl* hat: ein Zeichen, welches blofs *das* ausdrückt, was die drei Worte „*eine ganze Zahl*" aussagen, ohne alle Rücksicht auf die *Gröfse* der Zahl. Es geschieht dann das Nöthige, wenn man dieses Zeichen *ohne alle weitere Unterscheidung* z. B. an die Stelle der verschiedenen Quotienten, oder anderer Zahlen setzt, von welchen nichts weiter ausgesagt werden *soll,* als dafs sie *ganze* Zahlen, nicht Brüche, irrationale Zahlen u. s. w. sind.

V. Da ein *Zeichen* an sich *willkürlich* ist, so könnte man, um den blofsen Begriff der ganzen Zahl z. B. bei den Quotienten auszudrücken, etwa des Buchstabens q oder Q sich bedienen. Allein dies Zeichen wäre nicht allgemein und nicht *ausschliefslich* genug, indem man zu sehr gewohnt ist, unter Buchstaben, die auch noch *anderswo* vorkommen können, einen oder mehrere auf irgend eine Weise *bestimmte* Zahlenwerthe sich vorzustellen; was hier *nicht* geschehen *soll.* Man mufs, um *nichts weiter* als den blofsen Begriff der *ganzen Zahl* zu bezeichnen, nothwendig einen Buchstaben nehmen, der nicht leicht auch noch in anderem Sinne gebraucht wird; und dann sogar festsetzen, dafs dieser Buchstabe *nie* zu irgend einer andern Bezeichnung gebraucht werden soll.

Zu diesem Zwecke scheint der deutsche Buchstab 𝔊, auch als der Anfangsbuchstab von „*Ganzes*" oder „*Ganze-Zahl*", passend. Einige französische Schriftsteller bedienen sich auf ähnliche Weise zur Bezeichnung des Begriffs der *ganzen Zahl* des Anfangsbuchstabs E des Wortes *entier.* Wir setzen daher fest:

Dafs der Buchstab 𝔊 ausschliefslich dazu dienen soll, eine ganze Zahl überall da zu bezeichnen, wo es auf die Gröfse der Zahl durchaus nicht ankommt.

VI. Wenn es also z. B. bei den Ausdrücken (2.), die zu der Untersuchung der Eigenschaften irgend einer Verbindung der ganzen Zahlen z_1, z_2, z_3, ... z_n mit einander und mit vielleicht noch anderen Zahlen in Beziehung auf die Zahl u dienten, auf die *Gröfse* der Quotienten q, q_2, q_3, ... q_n *nicht* ankäme, sondern nur darauf, dafs sie *ganze* Zahlen sind, so würde man statt der *verschiedenen* q in (2.) *gleichmäfsig* 𝔊 und folglich, statt wie in (2.), blofs

$$3. \quad \begin{cases} z_1 = \mathfrak{G}u + r_1, \\ z_2 = \mathfrak{G}u + r_2, \\ z_3 = \mathfrak{G}u + r_3, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ z_n = \mathfrak{G}u + r_n \end{cases}$$

zu schreiben haben, wo nun ***einer und derselbe Buchstabe*** $\mathfrak{G}$ alle die verschiedenen Werthe von q *gleichzeitig* ausdrückt, oder wo vielmehr an die *Gröfse* der *ganzen* Zahlen, die $\mathfrak{G}$ bezeichnet, gar nicht mehr gedacht wird, sondern nur daran, *dafs* $\mathfrak{G}$ jedesmal eine *ganze* Zahl sein soll. Der Nutzen von Dergleichen wird sich in Dem was folgt zeigen.

VII. Diese Art des Gebrauchs eines Buchstabens, um Gröfsen oder Zahlen zu bezeichnen, ist zwar sonst nicht ganz gewöhnlich. Sie ist, wenn man will, etwas für die Theorie der Zahlen *Eigenthümliches*. Indessen ist einestheils das $\mathfrak{G}$ auch fast das *einzige* Eigenthümliche, was die Zahlentheorie in Anspruch nimmt, und fast alle übrigen Bezeichnungen und Operationen derselben sind ganz die nemlichen, wie in den übrigen Theilen des Calculs: anderntheils aber ist die Eigenthümlichkeit der Bezeichnungsart im Grunde doch *weniger* abweichend und vereinzelt, als sie es beim ersten Anblick zu sein scheint. Sie ist gewissermafsen nur eine Art von *Verallgemeinerung* des Gewöhnlichen; denn die Buchstaben überhaupt bezeichnen *gewöhnlich* schon *beliebige* Zahlen oder Gröfsen. Hier werden blofs noch die *Unterscheidungen* weggelassen, die man sonst zwischen den *Buchstaben* durch ihre Verschiedenheit oder durch Accente und dergleichen macht, weil die Unterscheidungen hier *nicht nöthig* sind.

VIII. Wenn nun in der Gleichung

$$4. \quad z = \mathfrak{G}u + r$$

$\mathfrak{G}$ in der angezeigten Bedeutung gebraucht wird, so nennt man eine solche Gleichung auch *Congruenz*.

Die beiden Zahlen z und r, deren Differenz $z - r$ oder $r - z$ durch u *theilbar* ist, indem (4.)

$$5. \quad z - r = \mathfrak{G}u \quad \text{und}$$

$$6. \quad r - z = -\mathfrak{G}u$$

giebt, für welches letztere man, da es auf die *Gröfse* von $\mathfrak{G}$ gar nicht ankommt, auch eben sowohl blofs

$$7. \quad r - z = \mathfrak{G}u$$

schreiben kann, und wo dann aus (5. u. 7.) hervorgeht, dafs $z - r$ und $r - z$

mit u *aufgehen*, weil $z-r$ und $r-z$ *Vielfache* von u, nemlich $\mathfrak{G}$fache sind, nennt man *zu einander congruent*.

Nicht congruent heifsen z und r, wenn $z-r$ oder $r-z$ *nicht* mit u aufgeht, also etwa

$$8. \quad z = \mathfrak{G}u + r + e$$

ist, wo e *nicht* mit u aufgeht, was

$$9. \quad z - r = \mathfrak{G}u + e \quad \text{und}$$

$$10. \quad r - z = \mathfrak{G}u - e$$

giebt und welches zeigt, dafs $z-r$ und $r-z$ *nicht* mit u aufgeht, indem solches der Voraussetzung nach mit e nicht der Fall ist.

Jede der beiden Zahlen z und r in (4.) nennt man *Residuum* der andern.

Den Divisor u nennt man auch *Modul*, und statt wie in (4.) schreibt man auch

$$11. \quad z \equiv r \text{ (mod. } u\text{)}.$$

Wir werden statt dieser letzten Art der Bezeichnung der Congruenzen die obige (4.) vermittels des $\mathfrak{G}$ beibehalten, weil dieselbe von Dem, was im übrigen Calcul gewöhnlich ist, weniger abweicht.

§. 11.

Lehrsatz.

Es bezeichne

$$1. \quad Z = F(z_1, z_2, z_3, \dots z_n)$$

von den ganzen Zahlen $z_1, z_2, z_3, \dots z_n$ *und von vielleicht noch andern ganzen Zahlen* $a_1, a_2, a_3, \dots b_1, b_2, b_3, \dots$ *etc., welche dieselben bleiben, wenn die* z *ihre Werthe ändern, irgend eine Verbindung, welche folgende zwei Eigenschaften hat:*

Erstlich, dafs für alle möglichen ganzzahligen Werthe der z, *so wie der* a, *der* b *etc.,* Z *selbst ebenfalls immer eine ganze Zahl ist, und*

Zweitens, dafs wenn man nach (§. 10.)

$$2. \quad \begin{cases} z_1 = \mathfrak{G}u + r_1, \\ z_2 = \mathfrak{G}u + r_2, \\ z_3 = \mathfrak{G}u + r_3, \\ \quad \cdot \quad \cdot \quad \cdot \\ z_n = \mathfrak{G}u + r_n \end{cases}$$

setzt, wo u, *und folglich die Reste* r, *ebenfalls lauter ganze Zahlen sind, darauf die Ausdrücke der* z (2.) *in* $F(z_1, z_2, z_3, \dots z_n)$ *substituirt und den daraus entstehenden Ausdruck von* Z *entwickelt, in diesem entwickel-*

ten Ausdrucke alle Glieder, in welchen u *vorkommt,* u *und ganze Zahlen* ***zu Factoren*** *haben und von den übrigen Gliedern, die* u ***nicht enthalten****, durch das Zeichen + oder — sich absondern lassen.*

Die sogenannten ***rationalen ganzen Functionen*** *oder* ***Verbindungen****, nemlich diejenigen, in welchen von den Zahlen* z, a, b, ... *nur Summen, Differenzen, Producte und Potenzen mit ganzzahligen positiven Exponenten vorkommen, nirgend Quotienten, Wurzelgröfsen, Exponentialgröfsen und andere transcendente Zahlen, haben jene beiden Eigenschaften; wie sich solches am besten an Beispielen zeigen wird.*

Für ***solche*** *Verbindungen* Z *gilt nun im Allgemeinen Folgendes.*

Wenn man nemlich in (1.) *statt der* z *ihre Ausdrücke* (2.) *setzt und den daraus entstehenden Ausdruck entwickelt, so hat derselbe immer die Form*

$$3. \quad Z = F(z_1, z_2, z_3, \ldots z_n) = \mathfrak{G}u + F(r_1, r_2, r_3, \ldots r_n);$$

das heifst, derjenige Theil $F(r_1, r_2, r_3, \ldots r_n)$ *des* ***entwickelten Ausdrucks*** *von* Z, *in welchem* ***kein*** u ***vorkommt****, hat genau* ***dieselbe Gestalt*** *wie* Z *selbst, blofs dafs überall* r *statt* z *steht; so dafs man also diesen Theil* ***unmittelbar*** *erhält, wenn man in* (1.) *blofs überall* r *statt* z *schreibt.*

Beweis. Nach der *Voraussetzung* soll Z (1.), wenn man darin die Ausdrücke der verschiedenen z aus (2.) setzt, entwickelt, die Form

$$4. \quad Z = F(\mathfrak{G}u + r_1, \mathfrak{G}u + r_2, \mathfrak{G}u + r_3, \ldots \mathfrak{G}u + r_n)$$
$$= u\varphi u + fr = \mathfrak{G}u + fr$$

haben, wo rechterhand der eine Theil $u\varphi u$ oder $\mathfrak{G}u$ des entwickelten Ausdrucks *durchweg* u *zum Factor hat,* der andere Theil fr *gar kein* u enthält.

Dieser Ausdruck gilt nun für alle möglichen ganzzahligen Werthe der z, und also auch für jeden ganzzahligen Werth von u; folglich auch für $u = 0$. Es ändert sich aber fr mit u *gar nicht,* weil es kein u enthält. Also bleibt in (4.) fr unverändert Dasselbe, auch wenn man $u = 0$ setzt, $u\varphi u$ hingegen verschwindet für $u = 0$, wegen des Factors u. Also giebt (4.), für $u = 0$.

$$5. \quad F(r_2, r_2, r_3, \ldots r_n) = fr,$$

und folglich ist in (4.), wenn man darin fr aus (5.) substituirt und statt $u\varphi u$ blofs $\mathfrak{G}u$ schreibt, welches letztere angeht, da nach der Voraussetzung u und φu *ganze* Zahlen sein sollen,

$$6. \quad Z = F(z_1, z_2, z_3, \ldots z_n) = \mathfrak{G}u + F(r_1, r_2, r_3, \ldots r_n);$$

wie es der Lehrsatz in (3.) behauptet.

Beispiele. *No. 1.* Es sei

$$7.\quad Z = a + a_1 z_1 + a_2 z_2 + a_3 z_3 \ldots. + a_n z_n,$$

wo die a beliebige positive oder negative ganze Zahlen sind, die nicht von z abhängen.

Setzt man hierin die Ausdrücke der z aus (2.), so erhält man

$$Z = a_0 + a_1(\mathfrak{S}u + r_1) + a_2(\mathfrak{S}u + r_2) + a_3(\mathfrak{S}u + r_3) \ldots. + a_n(\mathfrak{S}u + r_n) \text{ oder}$$
$$Z = u[a_1\mathfrak{S} + a_2\mathfrak{S} + a_3\mathfrak{S} \ldots. + a_n\mathfrak{S}] + a_0 + a_1 r_1 + a_2 r_2 + a_3 r_3 \ldots. + a_n r_n \text{ oder}$$
$$8.\quad Z = \mathfrak{S}u + a_0 + a_1 r_1 + a_2 r_2 + a_3 r_3 \ldots. + a_n r_n;$$

denn was in a multiplicirt ist sind lauter ganze Zahlen

Wie man sieht, besteht dieses Resultat aus zwei Theilen, deren einer die Form $\mathfrak{S}u$ hat, der andere unmittelbar aus Z (7.) hervorgeht, wenn man darin r statt z schreibt.

No. 2. Es sei

$$9.\quad Z = z_1 z_2,$$

so erhält man, wenn man die Ausdrücke (2.) der z substituirt:

$$10.\quad Z = (\mathfrak{S}u + r_1)(\mathfrak{S}u + r_2),$$

also, wenn man rechterhand die Factoren in einander multiplicirt,

$$Z = \mathfrak{S}\mathfrak{S}u^2 + \mathfrak{S}u.r_2 + \mathfrak{S}u.r_1 + r_1 r_2 \text{ oder}$$
$$Z = u[\mathfrak{S}\mathfrak{S}u + \mathfrak{S}r_2 + \mathfrak{S}r_1] + r_1 r_2 \text{ oder}$$
$$11.\quad Z = \mathfrak{S}u + r_1 r_2;$$

denn was in u multiplicirt ist, sind wieder lauter ganze Zahlen.

Das Resultat besteht wieder aus zwei Theilen, deren einer die Form $\mathfrak{S}u$ hat, der andere unmittelbar aus (9.) hervorgeht, wenn man r statt z schreibt.

No. 3. Es sei

$$12.\quad Z = z_1 z_2 z_3 \ldots. z_m.$$

Für $Z = z_1 z_2$ war $Z = \mathfrak{S}u + r_1 r_2$ (11.), also ist für $Z = z_1 z_2 z_3$, $Z = (\mathfrak{S}u + r_1 r_2)(\mathfrak{S}u + r_3)$. Dieses giebt, wenn man multiplicirt, auf ganz ähnliche Weise wie in (10.), $Z = \mathfrak{S}u + r_1 r_2 r_3$. Daraus folgt weiter für $Z = z_1 z_2 z_3 z_4$, $Z = (\mathfrak{S}u + r_1 r_2 r_3)(\mathfrak{S}u + r_4)$, und wieder auf ähnliche Art wie in (10.), $Z = \mathfrak{S}u + r_1 r_2 r_3 r_4$, und so immer weiter bis

$$13.\quad Z = \mathfrak{S}u + r_1 r_2 r_3 \ldots. r_m.$$

Auch hier ist der eine Theil des Resultats von der Form $\mathfrak{S}u$, der andere geht unmittelbar aus (12.) hervor, wenn man r statt z schreibt.

6 *

No. 4. Es sei

$$14.\quad Z = (a_0 + a_1 z_1 + a_2 z_2 \ldots\ldots + a_{n_1} z_{n_1})$$
$$\times (b_0 + b_1 z_1 + b_2 z_2 \ldots\ldots + b_{n_2} z_{n_2})$$
$$\times (c_0 + c_1 z_1 + c_2 z_2 \ldots\ldots + c_{n_3} z_{n_3})$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\times (m_0 + m_1 z_1 + m_2 z_2 \ldots\ldots + m_{n_n} z_{n_n}).$$

Der Kürze wegen bezeichne man die Factoren rechterhand der Reihe nach durch $\varphi_1 z$, $\varphi_2 z$, $\varphi_3 z$, ... $\varphi_m z$, so dafs

$$15.\quad Z = \varphi_1 z \,.\, \varphi_2 z \,.\, \varphi_3 z \ldots\ldots \varphi_m z$$

ist. Setzt man hierin die Ausdrücke (2.) von z, so geht, da die Factoren φz ganz die Form von (7.) haben, zufolge (No. 1.)

16. $\varphi_1 z$ in $\mathfrak{S}u + \varphi_1 r$, $\varphi_2 z$ in $\mathfrak{S}u + \varphi_2 r$, $\varphi_3 z$ in $\mathfrak{S}u + \varphi_3 r$ u. s. w.

über; also Z (15.) in

$$17.\quad Z = (\mathfrak{S}u + \varphi_1 r)(\mathfrak{S}u + \varphi_2 r)(\mathfrak{S}u + \varphi_3 r) \ldots\ldots (\mathfrak{S}u + \varphi_m r).$$

Man stelle sich vor, in (12. No. 3.) wären für die z, statt wie dort die Ausdrücke (2.), vielmehr der Reihe nach $z_1 = \mathfrak{S}u + \varphi_1 r$, $z_2 = \mathfrak{S}u + \varphi_2 r$, $z_3 = \mathfrak{S}u + \varphi_3 r$ u. s. w. gesetzt worden, so würden dort $\varphi_1 r$, $\varphi_2 r$, $\varphi_3 r$ etc. die Stellen von r_1, r_2, r_3 .... eingenommen haben. Also würde das Resultat, statt desjenigen (13.),

$$18.\quad Z = \mathfrak{S}u + \varphi_1 r \,.\, \varphi_2 r \,.\, \varphi_3 r \ldots\ldots \varphi_m r$$

gewesen sein. Dieses also ist das gegenwärtige zu (15.) oder (14.) gehörige Resultat. Auch dieses besteht aus einem Theil von der Form $\mathfrak{S}u$, und einem andern, der unmittelbar aus Z hervorgeht, wenn man darin r statt z schreibt.

No. 5. Es sei

$$19.\quad Z = z^m,$$

wo m irgend eine *ganze positive* Zahl ist.

Da diese Potenz z^m nichts anderes ist, als das Product von m Factoren, jeder gleich z. so erhält man was sich ergiebt, wenn man $\mathfrak{S}u + r$ statt z schreibt, unmittelbar aus (No. 3.), wenn man dort $z_1 = z_2 = z_3 \ldots\ldots = z_m = z$ und also auch $r_1 = r_2 = r_3 \ldots\ldots = r_m = r$ setzt. Das Resultat ist also

$$20.\quad Z = \mathfrak{S}u + r^m.$$

Dasselbe besteht wieder aus einem Theile von der Form $\mathfrak{S}u$, und einem andern, der unmittelbar aus (19.) sich ergiebt, wenn man r statt z setzt.

No. 6. Es sei

$$21.\quad Z = F(z_1, z_2, z_3, \ldots\ldots z_m) = z_1^{m_1} . z_2^{m_2} . z_3^{m_3} \ldots\ldots z_n^{m_n}.$$

Setzt man hierin die Ausdrücke der z aus (2), so geht zufolge (No. 5.) Z in

$$22.\quad Z = (\mathfrak{G}u + r_1^{m_1})(\mathfrak{G}u + r_2^{m_2})(\mathfrak{G}u + r_3^{m_3}) \dots (\mathfrak{G}u + r_n^{m_n})$$

über; und ganz auf ähnliche Weise wie in (No. 3.) findet sich, dafs das Product rechterhand, und folglich Z, nichts anderes ist als

$$23.\quad Z = \mathfrak{G}u + r_1^{m_1}.r_2^{m_2}.r_3^{m_3} \dots r_n^{m_n}.$$

Das Resultat ist, wie man sieht, wieder von der Form $\mathfrak{G}u + Fr$.

Ähnliches wird man immer finden, wenn auch Z eine noch mehr zusammengesetzte *ganze rationale* Verbindung ist; z. B. wenn in (14.) an der Stelle der verschiedenen z Producte verschiedener Potenzen der z wie (21.) stehen, u. s. w.

Anm. Zu bemerken ist, dafs der Lehrsatz durchaus *nur dann* unbedingt gilt, wenn die obigen *beiden Bedingungen* für Z erfüllt werden, und also nur für *ganze rationale* Verbindungen. Schon z. B. für

$$24.\quad Z = \frac{a+z}{b+z} = Fz$$

ist, wenn man $z = \mathfrak{G}u + r$ setzt, nicht nothwendig

$$25.\quad Z = \mathfrak{G}u + \frac{a+r}{b+r} = \mathfrak{G}u + Fr,$$

das heifst

$$26.\quad \frac{a+z}{b+z} - \frac{a+r}{b+r} = \mathfrak{G}u;$$

denn es folgt keinesweges, dafs der *Bruch* $\frac{a+z}{b+z}$ von dem Bruch $\frac{a+r}{b+r}$ für *jeden beliebigen* Werth von z und r um eine *ganze* Zahl, geschweige denn grade um ein Vielfaches $\mathfrak{G}u$ von u verschieden sei.

Anm. Der Rest $F(r_1, r_2, r_3, \dots r_n)$ (3.) von $Z = F(z_1, z_2, z_3, \dots z_n)$ zu dem Quotienten u ist übrigens nicht nothwendig ein *echter* Rest von Z zu u; selbst dann nicht, wenn die r in (2.) sämmtlich *echte* Reste zu den z sind; denn $F(r_1, r_2, r_3, \dots r_n)$ kann *viel gröfser* sein als u. Auch ist es, wenn man einen echten Rest zu Z haben will, keineswegs nöthig, erst $F(r_1, r_2, r_3, \dots r_n)$ wirklich zu berechnen, sondern man kann dazu in den einzelnen Fällen vermittels *kleinerer* Zahlen gelangen.

Anstatt nemlich z. B. in (8.) den Rest $a_0 + a_1 r_1 + a_2 r_2 \dots + a_n r_n$ ganz zu berechnen, nehme man erst die *echten* Reste zu a_0 und $a_1 r_1$ und ihre *Summe*. Ist diese Summe gröfser als u, so nehme man von ihr wieder erst den *echten* Rest, thue ihn zu demjenigen von $a_2 r_2$, verfahre mit der Summe wie vorhin, thue den echten Rest von $a_3 r_3$ hinzu, u. s. w. bis zu Ende. Dadurch werden

beständig noch *Vielfache von* u abgesondert, die zu $\mathfrak{G}u$ geschlagen werden können, und man gelangt zu dem *echten Rest* von Z vermittels *kleinerer* Zahlen.

Anstatt in (12.) das Product $r_1, r_2, r_3, \ldots r_m$ zu berechnen und davon den echten Rest nach u zu nehmen, berechne man erst den *echten* Rest zu $r_1 r_2$, multiplicire ihn mit r_3, nehme von dem Product den *echten* Rest, multiplicire diesen mit r_4, nehme wieder von dem Product den *echten* Rest, u. s. w. bis zu Ende, so gelangt man zu dem *echten* Rest von $Z = z_1, z_2, z_3, \ldots z_m$ wieder vermittels *kleinerer* Zahlen.

Wäre z. B. der *echte positive* Rest des Products

$$27. \quad Z = 18.25.41.61.123.191$$

zu der Zahl 13 zu berechnen, so ist nach (2.)

$$28. \quad \begin{cases} 18 = \mathfrak{G}.13+ 5, \\ 25 = \mathfrak{G}.13+12, \\ 41 = \mathfrak{G}.13+ 2, \\ 64 = \mathfrak{G}.13+12, \\ 123 = \mathfrak{G}.13+ 6, \\ 191 = \mathfrak{G}.13+ 9, \end{cases}$$

und nach (13.)

$$29. \quad Z = \mathfrak{G}.13+5.12.2.12.6.9.$$

Aber das Product 5.12.2.12.6.9 ist keineswegs der echte positive Rest von Z zu $u = 13$, obgleich alle r in (28.) *positive echte* Reste zu den z sind. Um den echten positiven Rest zu Z zu finden, nehme man erst $r_1 r_2 = 5.12 = \mathfrak{G}.13+8$, multiplicire dies mit $r_3 = 2$, welches $r_1 r_2 r_3 = 2(\mathfrak{G}.13+8) = \mathfrak{G}.13+16 = \mathfrak{G}.13+13+3 = \mathfrak{G}13+3$ giebt. Dieses multiplicirte man mit $r_4 = 12$, so erhält man $r_1 r_2 r_3 r_4 = 12(\mathfrak{G}.13+3) = \mathfrak{G}13+36 = \mathfrak{G}13+2.13+10 = \mathfrak{G}.13+10$. Dieses multiplicire man mit $r_5 = 6$, so ergiebt sich $r_1 r_2 r_3 r_4 r_5 = 6(\mathfrak{G}.13+10) = \mathfrak{G}13+60 = \mathfrak{G}13+4.13+.8 = \mathfrak{G}13+8$. Dieses endlich mit $r_6 = 9$ multiplicirt, giebt $9(\mathfrak{G}13+8) = \mathfrak{G}13+72 = \mathfrak{G}13+5.13+7 = \mathfrak{G}13+7$. Also ist

$$30. \quad r_1 r_2 r_2 r_3 r_4 r_5 r_6 = \mathfrak{G}13+7$$

und vermöge (29.)

$$31. \quad Z = \mathfrak{G}.13+\mathfrak{G}13+7 = \mathfrak{G}13+7,$$

und folglich ist 7 der *echte positive* Rest von Z (27.) zu $u = 13$.

Verlangt man den *unbedingt echten* Rest von Z (27.), so kann man auch sogleich die *unbedingt echten* Reste der Factoren z nehmen; welches *noch kleinere* Zahlen giebt. Es ist nemlich z. B. alsdann statt (28.)

$$32. \quad \begin{cases} 18 = \mathfrak{S}.13+5, \\ 25 = \mathfrak{S}.13-1, \\ 41 = \mathfrak{S}.13+2, \\ 64 = \mathfrak{S}.13-1, \\ 123 = \mathfrak{S}.13+6, \\ 191 = \mathfrak{S}.13-4. \end{cases}$$

Hier ist $r_1 r_2 = \mathfrak{S}13-5.1 = \mathfrak{S}13-5$. Dieses, mit $r_3 = 2$ multiplicirt, giebt $r_1 r_2 r_3 = 2(\mathfrak{S}13-5) = \mathfrak{S}13-10 = \mathfrak{S}13+3$. Dieses, mit $r_4 = -1$ multiplicirt, giebt $r_1 r_2 r_3 r_4 = -1(\mathfrak{S}13+3) = \mathfrak{S}13-3$. Dies, mit $r_5 = 6$ multiplicirt, giebt $r_1 r_2 r_3 r_4 r_5 = 6(\mathfrak{S}13-3) = \mathfrak{S}13-18 = \mathfrak{S}13-5$, und dieses, mit $r_6 = -4$ multiplicirt, giebt $-4(\mathfrak{S}13-5) = \mathfrak{S}13+20 = \mathfrak{S}13-6$; so dafs der *unbedingt echte* Rest von Z (27.) zu u, -6 ist.

§. 12.

Erklärungen und Erläuterungen.

I. Ganze Zahlen, die mit keiner andern ganzen Zahl >1 als mit sich selbst aufgehen, wie z. B. die Zahlen 2, 3, 5, 7, ... 53, 157, ... 353 u. s. w. kann man *Stammzahlen* nennen, weil die übrigen aus ihnen durch Multiplication zusammengesetzt werden können, und also von ihnen *abstammen*. Gewöhnlich heifsen sie *Primzahlen*. Noch besser, als eine *bildliche* deutsche oder fremde Benennung, wäre die geradezu *bezeichnende* Benennung *theilerlose* oder *untheilbare Zahlen*. Doch ist *Stammzahl* kürzer.

II. Ganze Zahlen, welche, aufser mit sich selbst, auch noch mit andern ganzen Zahlen >1 aufgehen, wie z. B. 15, was mit 3 und 5; 84, was mit 2, 3, 4, 6, 7, 12, 14, 21, 28 und 42 aufgeht u. s. w., nennt man gewöhnlich *zusammengesetzte Zahlen*. Kürzer und bezeichnender ist *theilbare Zahlen*. Zwar liefse sich dagegen sagen, dafs Zahlen auch noch auf andere Weise als durch Division theilbar sind, nemlich durch Subtraction; was auch selbst bei den Stammzahlen der Fall ist. Aber der Einwand trifft auch eben sowohl die Benennung *zusammengesetzte* Zahl; denn nicht blofs durch Multiplication, sondern auch durch Addition können Zahlen aus andern *zusammengesetzt* werden. *Theilbare Zahl* aber ist *kürzer*, und dürfte also besser sein. Man darf nur das Wort *theilen* ausschliefslich der *Division* vorbehalten und statt Theilen durch Subtraction *zerlegen* setzen, so ist die Benennung *theilbare Zahl* vollständig und ausschliefslich *bezeichnend*.

III. Zwei ganze Zahlen, welche mit keiner ganzen Zahl >1 *beide zugleich* aufgehen, und die also einander rücksichtlich ihrer Theilbarkeit oder ihrer Theiler *fremd* sind, wie z. B. 8 und 15, 165 und 238 u. s. w., nennt man gewöhnlich *relative Primzahlen.* Natürlicher wäre es, sie geradezu, nach ihrer vorhin bezeichneten Eigenschaft, *theilerfremde Zahlen* zu nennen. Alle Stammzahlen sind einander *theilerfremd.*

IV. Zweien oder mehreren Zahlen, welche mit andern ganzen Zahlen >1 *zugleich* aufgehen, z. B. 105 und 154, die mit 7; 66 und 102, die mit 2, 3 und 6; 30, 105 und 195, die mit 3. 5 und 15 aufgehen u. s. w. pflegt man gewöhnlich nicht eigentlich eine besondere Benennung beizulegen. Natürlich wäre es indessen, solche Zahlen, im Gegensatz zu den *theilerfremden* Zahlen, *theilerverwandte* Zahlen zu nennen. Die Beiwörter *theilerverwandt* und *theilerfremd* dürften andern, ganz gebräuchlichen, zu ähnlichen Zwecken zusammengesetzten Beiwörtern, z. B. den Beiwörtern *sinnverwandt* und *sinnfremd*, als nachgebildet zu betrachten und also *grammatisch* nicht zu verwerfen sein.

V. Diejenigen ganzen Zahlen >1, welche in zwei oder mehrere ganze Zahlen *zugleich* aufgehen, nennt man ihre *gemeinschaftlichen* Theiler und die gröfste unter ihnen *gröfsten gemeinschaftlichen Theiler.* Kürzer wäre *Gemeintheiler* und *gröfster Gemeintheiler;* nach dem Vorbilde z. B. des Wortes *Gemeingut.*

VI. Für mehr als *zwei* Zahlen reicht die Benennung *theilerfremd* nicht aus, um alles was nöthig ist auszudrücken; die Benennung *relative Primzahl* ebenso wenig. Denn es können Zahlen, wenn ihrer mehr als zwei sind, ohne *gemeinschaftliche* Theiler sein, während sie gleichwohl *nicht* relative Primzahlen sind. Zum Beispiel die 6 Zahlen $198 = 2.3^2.11$, $165 = 3.5.11$, $255 = 3.5.17$, $154 = 2.7.11$, $228 = 2^2.3.19$ und $715 = 5.11.13$ haben *keinen gemeinschaftlichen* Theiler: gleichwohl ist *keine* zu der andern relative Primzahl, sondern 198 hat mit 165, 255 und 228 den Theiler 3, mit 154 und 228 den Theiler 2, mit 165, 154 und 715 den Theiler 11 gemein u. s. w. Man kann also solche Zahlen weder theilerfremd noch relative Primzahlen nennen. Die Benennung für sie ergiebt sich aber aus (V.) von selbst. Sie haben nemlich keinen *Gemeintheiler* und müssen folglich *gemeintheilerfremd* heifsen. *Zwei* Zahlen, wenn sie theilerfremd sind, sind auch gemeintheilerfremd, und daher genügt für *zwei* Zahlen die Benennung *theilerfremd.*

Mehr als zwei Zahlen dagegen können gleichzeitig *gemeintheilerfremd* und *theilerverwandt* sein.

VII. Haben mehr als zwei Zahlen *Gemeintheiler,* wie z. B. 198, 165, 255 und 228, die alle mit 3 aufgehen, so werden sie *gemeintheilerverwandt* heifsen müssen. Dergleichen Zahlen sind natürlich auch immer *theilerverwandt.* Für blofs zwei Zahlen genügt *theilerverwandt;* denn sind sie das, so sind sie auch *gemeintheilerverwandt.*

VIII. Zwei ganze Zahlen, deren Summe oder Differenz mit einer bestimmten dritten ganzen Zahl aufgeht, wie z. B. die Zahlen z und r in der Gleichung $z = \mathfrak{G}u \pm r$, deren Summe oder Differenz $z \pm r$ mit der Zahl u aufgeht, und die man gewöhnlich nach (§. 10. VIII.) *zu einander nach dem Modul u congruent* nennt, könnte man deutsch *zu einander nach dem Theiler u theilbar* nennen. Das Wort *zu* würde das Zueinanderhinzuthun der beiden Zahlen andeuten.

IX. Je nachdem Zähler und Nenner eines Bruches *theilerfremd* oder *theilerverwandt* sind, nennt man gewöhnlich den Bruch *irreducibel* oder *reducibel,* und das Wegschaffen der Gemeintheiler von Zähler und Nenner *Reduciren* des Bruchs. Gegenbildlich zu den allgemein gebräuchlichen Benennungen *echter* und *unechter* Bruch, könnte man irreducible Brüche *reine,* reducible *unreine* nennen. Statt *reduciren* könnte es heifsen: einen Bruch *aufheben* oder, wenn man will, *reinigen.*

X. Sind die ganzzahligen Factoren einer Zahl untheilbar oder Stammzahlen, so heifsen sie folgerichtig *Stammfactoren.*

Besser als bildliche oder willkürliche Benennungen sind unstreitig überall, und folglich auch, und sogar ganz besonders in der *Mathematik,* solche Benennungen, die ihren Gegenstand möglichst gradezu bezeichnen; denn sie begünstigen weniger die Verwechselungen. Es ist zweifelsohne überall gut, die Dinge bei ihrem rechten Namen zu nennen.

Sodann sind wohl unstreitig Benennungen aus der Sprache selbst, in welcher man sich ausdrückt, schon im Allgemeinen besser, als Benennungen aus andern Sprachen; denn sie verstärken die Deutlichkeit und Verständlichkeit der Rede. Sind die Benennungen aus der eigenen Sprache *eben so* bezeichnend, oder bezeichnender als die fremden, so ist es gradezu *unrecht,* die letztern statt jener zu setzen; denn es kann dann nur aus *Verachtung* der

eigenen Sprache geschehen; und zu dieser haben die Deutschen wohl ebenso wenig, wie irgend ein anderes Volk, Ursach.

Es ist zwar nicht unwahrscheinlich, dafs *alle* fremden Benennungen, auch in der Mathematik, durch deutsche sich ersetzen lassen; und wären selbst nur *bildliche* Benennungen zu finden, so wären sie, als spracheigen, gleichwohl noch besser, als die fremden, insofern diese ebenfalls, wie z. B. die fremden Wörter Product, Factor, Sinus, Cosinus, positiv, negativ, rational, irrational, Factorielle, Facultät, Differential, Integral u. s. w., nur bildlich sind. Indessen ist es gewifs gut, die Verdeutschung *solcher* Ausdrücke mehr der Zeit zu überlassen, weil das, was nicht zugleich *in sich* entschieden besser ist, als das Fremde, durch seine Heimathlichkeit allein vielleicht nicht Recht genug hat, das in Besitz begriffene Fremde zu vertreiben. Wo dagegen völlig *bezeichnende* deutsche Benennungen ganz bereit zur Hand sind, haben sie *volles Recht,* die Stelle der fremden einzunehmen.

Dafs übrigens etwa die Einführung weniger oder gar noch nicht gewöhnlicher Benennungen das Studium einer Wissenschaft erschweren werde, ist nicht zu fürchten, sobald nur die neuen Worte ihre Gegenstände mehr beim rechten Namen nennen, als die alten, oder auch nur für ähnliche Begriffe schon gäng und gebe sind. Das Ungewohnte darf nur allein dann zurückgewiesen werden, wenn es in sich *weniger gut* ist, als das Gewohnte; *niemals* wenn es *besser* ist.

In diesen Erwägungen liegen die Gründe zu den Aufstellungen des gegenwärtigen Paragraphs. Die Absicht, deutsche Worte, welche bezeichnender sein mögen, als die gewöhnlichen fremden, für einige Gegenstände der vorliegenden Abhandlung statt der fremden zu setzen, ist übrigens auch den Erfolgen, die die Erfahrung längst ergeben hat, nicht entgegen. Auch in der Mathematik sind in der neuern Zeit schon statt *vieler* fremden Worte deutsche ziemlich allgemein angenommen worden; z. B. Unterschied statt Differenz, Vielfaches statt Multiplum, Verhältnifs statt Proportion, Reihe statt Progression, Dreieck, Viereck, Vieleck, Kegel, Kugel, statt Triangel, Quadrangel, Polygon, Conus, Sphaere u. s. w. Es ist also hier in diesem Paragraph nur etwas geschehen, was dem *erfahrungsmäfsig* wirklich stattfindenden Bestreben *gemäfs* ist: nichts, was ihm *entgegen* wäre. Daher werden wir uns der hier aufgestellten Benennungen in Dem was folgt statt der sonst gewöhnlichen bedienen.

§. 13.

Erläuterung.

A. Eine ***ganze Zahl*** drückt die Gröfse der ***Menge*** von einzelnen Dingen aus, welche man, indem man sie zusammenfafst, in irgend einer Beziehung als unter einander ***gleich*** betrachtet. Die Zahl für ein einzelnes Ding ist die ***Einheit.*** ***Ziffern*** sind die Zeichen für ganze Zahlen, wenn die Gröfse der Mengen ***bestimmt*** ist; ***Buchstaben,*** oder beliebige andere Zeichen sind es, wenn die Gröfse der Mengen ***unbestimmt*** ist.

B. Für den Begriff der Gröfse der Menge an sich, oder der Zahl, ist es offenbar völlig gleichgültig, ***welche*** Dinge es sind, deren Menge die Zahl vorstellt. In diesem Sinne ist es ***nicht*** angemessen, eine Zahl, ***ohne*** Rücksicht auf die Dinge welche sie ***zählt, unbenannte*** Zahl, und dagegen die Gesammtheit der Dinge ***selbst,*** welche die Zahl zusammenfafst, ***benannte Zahl*** zu nennen. Die Dinge ***selbst*** können niemals eine ***Zahl*** sein; es kann immer nur heifsen: eine Zahl ***benannter Dinge.*** Der Begriff der Zahl ist abstract, oder von den Dingen, auf welche er angewendet wird, ***abgezogen.*** Er liegt nicht ***in*** den Dingen, sondern wird auf sie ***angewendet.***

C. Es können aber nicht blofs Dinge, die in irgend einer Beziehung als unter einander gleich betrachtet werden, zu zählen sein, sondern es können auch Dinge, wenn sie beliebig ***theilbar*** sind, in ***Theile*** zu ***theilen*** sein, die ihrerseits unter sich in irgend einer Beziehung als gleich betrachtet werden. Es ist also zunächst auch noch auszudrücken nöthig, in ***wieviele*** gleiche Theile etwa ein Ding, welches als Einheit betrachtet wird, zu theilen sei; und dann, wieviele ***solcher Theile*** genommen werden sollen. Da es hier wiederum nur auf die Gröfse von ***Mengen*** ankommt, nemlich erstlich auf die ***Menge*** der ***gleichen Theile,*** welche ***ein einzelnes Ding ausmachen*** sollen, und dann zweitens auf die ***Menge*** dieser ***Theile,*** welche zu nehmen sind, so kann beides ebenfalls durch die ***Zahl*** geschehen. Wie man die Zahlen, welche hier das Verlangte anzeigen, zu einander stellen will, ist ***willkürlich.*** Man schreibt, wenn z. B. ein Ding in b gleiche Theile zu theilen ist und a solcher Theile genommen werden sollen, wo dann a und b Zeichen ***ganzer*** Zahlen sind,

$$1. \quad \frac{a}{b} \text{ oder auch } a:b,$$

und nennt diesen Zahlen-Ausdruck ***Bruch,*** a den ***Zähler,*** b den ***Nenner*** des Bruchs.

D. Brüche und ganze Zahlen reichen für *alle* Fälle, welche in der Rechnung vorkommen können, *vollständig* aus; denn auch Irrationales, so wie Transcendentes, sind nur *Grenzen* gewisser nach diesem oder jenem Gesetz sich richtender *Brüche;* und selbst Imaginäres geht nur erst aus der Rechnung mit Zahlen hervor.

Da nun Brüche eben sowohl *Mengen zählen,* als ganze Zahlen, nemlich *Theile* von Dingen, die als neue Einheiten betrachtet werden, so kann man füglich die Bedeutung des Worts *Zahl verallgemeinern,* und es eben sowohl ganze Zahlen, als Brüche ausdrücken lassen. Mengen von *Einheiten* heifsen dann *ganze Zahlen,* Mengen von *Theilen* von Einheiten *Brüche;* beide gleichmäfsig *Zahlen.* Darstellbar sind Brüche durch ganze Zahlen immer.

E. Da $\frac{a}{b}$ nach (*C.*) a gleiche Theile bezeichnet, deren b die Einheit ausmachen, so drückt $\frac{1}{b}$ *einen* dieser Theile aus: denn für *einen* solchen Theil ist der *Zähler* a der Theile gleich 1. Also bezeichnet $a.\frac{1}{b}$ *dasselbe,* wie $\frac{a}{b}$, und folglich ist

$$2. \quad \frac{a}{b} = a.\frac{1}{b}.$$

F. Auch kommt offenbar Dasselbe heraus, ob man die Einheit in b Theile theilt und a solcher Theile nimmt, oder ob man a Einheiten als ein *Ganzes* betrachtet und dieses Ganze in b Theile theilt: denn, so wie a *Einheiten* das Ganze a zusammensetzen, so setzen auch, *nach der Theilung* des Ganzen a in b Theile, a einzelne *Theile* der Einheit, jeder $= \frac{1}{b}$, den $b$ten Theil $\frac{a}{b}$ des Ganzen a zusammen. Also kann man sich $\frac{a}{b}$ statt als a $b$te Theile der Einheit, auch als den $b$ten Theil des Ganzen a vorstellen.

G. Wenn $\frac{a}{b}$ mit der ganzen Zahl c zu *multipliciren* ist, was durch $c.\frac{a}{b}$ auszudrücken sein wird, so folgt zunächst aus (2.)

$$3. \quad c.\frac{a}{b} = c.a.\frac{1}{b}.$$

das heifst, rechterhand: a Dinge oder Einheiten, jedes $= \frac{1}{b}$, sind $c$mal zu nehmen. Aber die ganze Zahl ca drückt eben soviel Einheiten aus als c*mal* a. Dieses ist kein zu *beweisender* sondern ein willkürlicher Satz. Erst dafs $ca = ac$ sei, oder dafs $a$mal c eben soviele Einheiten enthält, als $c$mal a,

ist ein des Beweises bedürfender Satz. Es ist derjenige (§. 6.), und er ist dort bewiesen.

Also kann statt (3.) auch geschrieben werden:

$$4.\quad c.\frac{a}{b} = ca.\frac{1}{b}.$$

Aber eben so wie $\frac{1}{b}$, mit der ganzen Zahl a multiplicirt, soviel ist als $\frac{a}{b}$ (2.), ist auch $\frac{1}{b}$ mit der ganzen Zahl ca multiplicirt soviel als $\frac{ca}{b}$. Also ist

$$5.\quad ca.\frac{1}{b} = \frac{ca}{b} = c.\frac{a}{b}.$$

H. Wenn der $b$te Theil der Einheit weiter in c gleiche Theile getheilt wird, so machen c solcher Theile $\frac{1}{b}$ aus. Nimmt man also statt c jener Theile, ihrer *bmal c*, so hat man das $b$fache des Resultats $\frac{1}{b}$. Dieses aber ist $= 1$. Also machen $b$mal c, oder, was dasselbe ist, bc jener $c$ten vom $b$ten Theile der Einheit die Einheit aus. Eben das ist mit dem bcten Theile der Einheit der Fall, also ist

$$6.\quad \frac{1}{b} : c = \frac{1}{bc}.$$

Auch ist demnach

$$7.\quad \frac{a}{b} : c = \frac{a}{bc};$$

denn $\frac{a}{b}$ ist $= a.\frac{1}{b}$ (2.), also $\frac{a}{b} : c = a.\frac{1}{b} : c = a.\frac{1}{bc}$ (6.) $= \frac{a}{bc}$ (2.).

I. Wenn $\frac{a}{bc}$ mit c zu multipliciren ist, welches durch $c.\frac{a}{bc}$ auszudrücken sein wird, so ist erstlich wegen $\frac{a}{bc} = a.\frac{1}{bc}$ (2.), $c.\frac{a}{bc} = c.a.\frac{1}{bc}$ $= a.c.\frac{1}{bc}$. Aber $\frac{1}{bc}$ kann man sich nach (6.) als $\frac{1}{b}$ *dividirt* durch c vorstellen. Da nun hier $\frac{1}{bc}$ oder $\frac{1}{b}$, *dividirt* durch c, wieder zunächst *cmal zu nehmen* ist, so giebt $c.\frac{1}{bc} = \frac{1}{b}$. Also ist $a.c.\frac{1}{bc} = a.\frac{1}{b}$ und dieses ist $= \frac{a}{b}$ (2.). Aber es ist $a.c.\frac{1}{bc} = ac.\frac{1}{bc} = \frac{ac}{bc}$ (2.): also ist

$$8.\quad \frac{ac}{bc} = \frac{a}{b};$$

das heifst: *gleiche* Factoren im Zähler und Nenner eines Bruchs *heben sich auf.* Diese nähere Erörterung wegen des *Aufhebens* der Factoren in Brüchen war des Folgenden wegen nöthig.

§. 14.

Lehrsatz.

I. ***Jede ganze Zahl geht nothwendig mit jedem ihrer ganzzahligen Factoren auf, das heifst: wenn man die Zahl durch den Factor dividirt, so ist der Quotient eine ganze Zahl; oder auch, wenn man den Factor wiederholt von der Zahl abzieht, so bleibt zuletzt Null.***

II. ***Jede ganze Zahl, die in eine andere ganze Zahl aufgeht, ist einer ihrer Factoren.***

III. ***Wenn der Quotient, z. B. der ganzen Zahl*** z, ***dividirt durch die ganze Zahl*** u, ***eine ganze Zahl*** w ***ist, so geht*** u ***in*** z ***nothwendig auf.***

Beweis von I. Es seien $u_1, u_2, u_3, \ldots u_n$ die verschiedenen ganzzahligen Factoren der ganzen Zahl z, so dafs

$$1. \quad z = u_1 . u_2 . u_3 \ldots u_n$$

ist. Da die u sämmtlich ganze Zahlen sind, so ist z. B. auch $u_2 . u_3 \ldots u_n$ eine ganze Zahl, folglich ist, wenn man dieselbe durch v bezeichnet

$$2. \quad z = u_1 . v.$$

Aus (2.) folgt, dafs der Factor u_1 v mal in z enthalten ist, also, v mal davon abgezogen, der Rest Null bleibt, oder dafs u_1 in z aufgeht. Gleiches gilt von jedem andern Factor von z.

Beweis von II. Wenn u_1 in z aufgeht, oder, z. B. v mal von z abgezogen, Null läfst, so ist z aus v mal u_1 zusammengesetzt, und folglich u_1 ein Factor von z.

Beweis von III. Wenn man

$$3. \quad \frac{z}{u} = w$$

setzt, so ist nach (§ 13. 5. *I.*)

$$4. \quad u . \frac{z}{u} \text{ oder } u . w = \frac{u . z}{u} = z.$$

Wenn also nun w eine *ganze* Zahl ist, so folgt aus (4.), dafs u eine ganze Zahl von Malen in z enthalten ist, also in z aufgeht.

§. 15.

Lehrsatz.

I. ***Wenn irgend ein Factor*** v_1 ***einer ganzen Zahl***

$$1. \quad u = v_1 . v_2 . v_3 \ldots v_n$$

in eine ganze Zahl z ***nicht aufgeht, so geht auch*** u ***selbst nicht in*** z ***auf.***

II. ***Wenn* u *in* z *aufgeht, so geht auch jeder Factor* v *von* u *in* z *auf.***

Beispiel zu I. Der Factor 3 der Zahl $u = 78 = 2.3.13$ geht in die Zahl $z = 1430 = 2.5.11.13$ *nicht* auf; und auch $u = 78$ geht in 1430 nicht auf, obgleich die übrigen Factoren 2, 13 und 26 in 1430 aufgehen.

Beispiel zu II. Die Zahl $u = 286 = 2.11.13$ geht in $z = 1430 = 2.5.11.13$ auf. Und auch alle die Factoren 2, 11, 13, 22, 26 und 143 von 286 gehen in 1430 auf.

Beweis von I. Man setze

$$2. \quad v_2.v_3.v_4 \ldots v_n = y,$$

so dafs in (1.)

$$3. \quad u = v_1.y \quad \text{und} \quad y = \frac{u}{v_1} \quad (\text{§. 14. I.})$$

ist. Ferner sei

$$4. \quad \frac{z}{v_1} = w_1 \quad \text{und}$$

$$5. \quad \frac{z}{u} \quad \text{oder} \quad \frac{z}{v_1.y} \; (3.) = w.$$

Man multiplicire (5.) mit y, so erhält man

$$6. \quad wy = y.\frac{z}{v_1 y} = \frac{yz}{v_1 y} = \frac{z}{v_1} \quad (\text{§. 13. } I.).$$

Daher ist, (6.) in (4.) gesetzt,

$$7. \quad w_1 = wy.$$

Nun geht nach der Voraussetzung v_1 in z *nicht* auf. Also ist zufolge (4.) w_1 *nicht* eine ganze Zahl. Gingen dagegen u in z auf, so wäre nach (5.) w eine *ganze* Zahl. Aber auch y (2.) ist eine ganze Zahl, und folglich auch wy, welches nach (7.) *gleich* w_1 sein soll. Also wäre eine ganze Zahl einer nicht ganzen Zahl gleich. Aus diesem Widerspruch folgt, dafs, wenn irgend ein Factor v_1 von u in z *nicht* aufgeht, auch u selbst nicht in z aufgehen kann.

Beweis von II. Wenn u in z aufgeht, so ist w (5.) eine ganze Zahl; desgleichen ist, wenn v_1 irgend einen Factor von u bezeichnet, y in (3.) eine ganze Zahl. Nun ist nach (§. 13. *I.*)

$$8. \quad u.\frac{z}{u} \quad \text{oder} \quad u.w = \frac{uz}{u} = z \quad \text{und}$$

$$9. \quad v.\frac{u}{v_1} \quad \text{oder} \quad v_1.y\,(3.) = \frac{v_1 u}{v_1} = u:$$

also, wenn man (9.) in (8.) setzt,

$$10. \quad z = v_1 y w.$$

Da nun nach der Voraussetzung w und y ganze Zahlen sind, so ist auch yw eine ganze Zahl, und folglich ist der Factor v_1 von u eine ganze Zahl yw von Malen in z enthalten, und geht folglich in z auf. Gleiches gilt von jedem andern Factor von u. Also geht jeder Factor von u in z auf, wenn u selbst in z aufgeht.

§. 16.

Lehrsatz.

Wenn eine ganze Zahl z *mit einer andern ganzen Zahl* u *aufgeht, so ist der Quotient der Division der nemliche, man mag* z *auf einmal mit* u *dividiren, oder erst durch irgend einen der Factoren* v_1 *von* u, *darauf den Quotienten dieser Division durch irgend einen andern Factor* v_2 *von* u, *den Quotienten hievon durch einen dritten Factor* v_3 *von* u *u. s. w. Nur mufs die zweite Art der Division so lange fortgesetzt werden, bis alle Factoren* v *von* u *erschöpft sind. Alle bei dieser zweiten Art der Division sich ergebenden Quotienten sind der Reihe nach ganze Zahlen. Die Ordnung, in welcher man bei dem zweiten Verfahren die Factoren* v *von* u *zu Divisoren nimmt, ist willkürlich. Auch bleibt der Satz unverändert derselbe, wenn die Factoren* v *von* u, *alle oder einige, unter einander gleich sind.*

Beispiel. $z = 84$, durch $u = 12 = 2.2.3$ auf einmal dividirt, giebt 7. Andrerseits ist

$$1. \quad \begin{cases} \frac{84}{2} = 42, & \frac{42}{2} = 21, \quad \frac{21}{3} = 7. \\ \frac{84}{3} = 28, & \frac{28}{4} = 7. \\ \frac{84}{6} = 14. & \frac{14}{2} = 7. \\ \frac{84}{4} = 21. & \frac{21}{3} = 7. \\ \frac{84}{2} = 42. & \frac{42}{6} = 7 \quad \text{u. s. w.} \end{cases}$$

Immer ist der letzte Quotient der nemliche, und alle darauf führenden Quotienten sind *ganze* Zahlen.

Beweis. *A.* Da *nach der Voraussetzung* z mit

$$2. \quad u = v_1 . v_2 . v_3 \ldots . v_x,$$

wo die v beliebige theilbare oder untheilbare Factoren von u sein können, aufgehen soll, so geht zufolge (§. 15. II.) z auch mit *jedem* dieser Factoren v von u auf.

B. Nun sind v_1, $v_1 v_2$, $v_1 v_2 v_3$, ... sämmtlich Factoren von u, also sind, wenn man

$$3.\quad \frac{z}{v_1} = w_1,\ \frac{z}{v_1 v_2} = w_2,\ \frac{z}{v_1 v_2 v_3} = w_3,\ \ldots\ \frac{z}{v_1 v_2 v_3 \ldots v_{k-1}} = w_{k-1},$$
$$\frac{z}{v_1 v_2 v_3 \ldots v_k} = w_k,\ \ldots\ \frac{z}{v_1 v_2 v_3 \ldots v_n} = \frac{z}{u} = w_n$$

setzt, alle die Quotienten w *ganze* Zahlen.

C. Die beiden vorletzten Gleichungen in (3.) geben, wenn man sie, die erste mit $v_1 v_2 v_3 \ldots v_{k-1}$, die zweite mit $v_1 v_2 v_3 \ldots v_k$ multiplicirt, zufolge (§. 13. *I.*)

$$4.\quad z = v_1 v_2 v_3 \ldots v_{k-1} w_{k-1} \text{ und}$$
$$5.\quad z = v_1 v_2 v_3 \ldots v_{k-1} v_k w_k,$$

also, (4.) durch (5.) dividirt,

$$6.\quad \frac{z}{z} = 1 = \frac{v_1 v_2 v_3 \ldots v_{k-1} w_{k-1}}{v_1 v_2 v_3 \ldots v_{k-1} v_k w_k} = \frac{w_{k-1}}{v_k w_k} \text{ (§. 13. } I.),$$

und dieses mit w_k multiplicirt, wiederum nach (§. 13. *I.*),

$$7.\quad \frac{w_{k-1}}{v_k} = w_k.$$

D. Da nun k jede der Zahlen 1, 2, 3, ... n sein kann, so giebt (7.)

$$8.\quad \frac{w_1}{v_2} = w_2,\ \frac{w_2}{v_3} = w_3,\ \frac{w_3}{v_4} = w_4,\ \ldots\ \frac{w_{n-1}}{v_n} = w_n.$$

Hieraus folgt

Erstlich, dafs jeder der Quotienten w der Division von z durch die Factoren v von u (3.) durch einen derjenigen Factoren v von u *theilbar* ist, die bis dahin noch nicht zur Division gekommen sind; denn die sämmtlichen Quotienten in (8.) sind ganze Zahlen (*B.*). So behauptet es der Lehrsatz.

Zweitens, dafs, wenn man zuerst z durch v_1 dividirt, welches den Quotienten w_1 giebt (3.), darauf diesen Quotienten w_1 durch v_2, den daraus nach (8.) hervorgehenden Quotienten w_2 durch v_3 u. s. w. bis *alle* Factoren v von u zur Division gelangt sind: dafs dann der *letzte* Quotient w_n der ***nemliche*** ist, welcher sich zufolge (3.) ergiebt, wenn man z *auf einmal* durch $v_1 v_2 v_3 \ldots v_n = u$ dividirt; dem Lehrsatze gemäfs.

E. Übrigens ist es gleichgültig, in welcher ***Ordnung*** die Factoren v von u bei dem zweiten Divisionsverfahren zur Division gelangen, da die Factoren v_1, v_2, v_3, ... v_n von u zufolge (§. 6.) nach Belieben ***verwechselt*** werden dürfen. Auch ändert sich an dem Beweise nichts, die Fac-

toren v von u mögen, einige oder alle, unter einander gleich oder ungleich sein; was die übrigen Behauptungen des Lehrsatzes sind.

Anm. Der Beweis ergiebt sich insbesondere aus der *Vergleichung* in (*C.*) zweier Quotienten w von z, dividirt durch Factoren von u, in welchen der Divisor des einen *einen* Factor von u mehr enthält, als der andere.

§. 17.

Lehrsatz.

Der Lehrsatz (§. 16.) von der Gleichheit der Endresultate, es mag eine ganze Zahl z *durch eine andere ganze Zahl* u *auf einmal, oder erst durch irgend einen Factor von* u, *der Quotient davon durch einen zweiten Factor von* u, *der Quotient davon durch einen dritten Factor von* u *dividirt werden u. s. w. bis alle Factoren von* u *erschöpft sind, gilt nicht blofs für den Fall, wenn* u *in* z *aufgeht, sondern auch dann, wenn* u *in* z *nicht aufgeht; jedoch dann nur auf folgende Weise:*

I. *Dividirt man nämlich in diesem Fall* z *zuerst durch irgend einen Factor* v_1 *von* u, *und zwar so, dafs das was bleibt entweder der echte positive oder der echte negative Rest* (§. 8. IV. *a.*) *ist; hierauf den so gefundenen unternächsten oder übernächsten Quotienten* (§. 8. IV. *b.*) *durch irgend einen zweiten Factor* v_2 *von* u, *unter der gleichen Beobachtung; den hieraus hervorgehenden Quotienten durch einen dritten Factor* v_3 *von* u, *wiederum unter derselben Beobachtung, und so weiter bis alle Factoren von* u *erschöpft sind, so kommt man, und zwar immer unter der Bedingung, dafs bei den stufenweisen Divisionen stets entweder der positive oder der negative echte Rest genommen wird (nicht willkürlich bald der eine, bald der andere), zuletzt auf denselben Quotienten, der sich findet, wenn man* z *durch* u *auf einmal dividirt und auch hierbei, eben wie bei den stufenweisen Divisionen, gleichfalls den positiven oder den negativen echten Rest nimmt, je nachdem der eine oder der andere bei den stufenweisen Divisionen genommen wurde.*

Bezeichnet man, indem

$$1.\quad u = v_1 v_2 v_3 \ldots\ldots v_n$$

gesetzt wird, die bei den verschiedenen theilweisen Divisionen bleibenden Reste, je nachdem sie die positiven oder die negativen echten Reste sind, durch $r_1, r_2, r_3, \ldots\ldots r_n$, *und durch* $r_1, r_2, r_3, \ldots\ldots r_n$, *die zugehöri-*



gen ***unternächsten*** *und* ***übernächsten*** *Quotienten durch* $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \ldots \mathfrak{q}_n$ *und durch* $q_1, q_2, q_3, \ldots q_n$; *ferner den* ***positiven echten*** *Rest der Division von* z *mit* u *durch* R, *den* ***negativen echten*** *Rest dieser Division durch* $\mathfrak{R}$, *die zugehörigen* ***unternächsten*** *und* ***übernächsten*** *Quotienten durch* Q *und* $\mathfrak{Q}$, *so dafs die Gleichungen*

$$2.\quad \begin{cases} z = \mathfrak{q}_1 v_1 + r_1, \\ \mathfrak{q}_1 = \mathfrak{q}_2 v_2 + r_2, \\ \mathfrak{q}_2 = \mathfrak{q}_3 v_3 + r_3, \\ \mathfrak{q}_3 = \mathfrak{q}_4 v_4 + r_4, \\ \ldots \\ \mathfrak{q}_{n-1} = \mathfrak{q}_n v_n + r_n, \end{cases} \qquad 3.\quad \begin{cases} z = q_1 v_1 - r_1, \\ q_1 = q_2 v_2 - r_2, \\ q_2 = q_3 v_3 - r_3, \\ q_3 = q_4 v_4 - r_4, \\ \ldots \\ q_{n-1} = q_n v_n - r_n, \end{cases}$$

und

$$4.\quad z = Qu + R \text{ und}$$
$$5.\quad z = \mathfrak{Q}u - \mathfrak{R}$$

die verschiedenen oben beschriebenen Divisionen vorstellen und die Quotienten $\mathfrak{q}$, Q *und* q, $\mathfrak{Q}$, *durch die Bezeichnungen* (§. 8. IV. *b.*) *ausgedrückt, nichts anderes sind als*

$$6.\quad \begin{cases} \mathfrak{q}_1 = (z +: v_1), \\ \mathfrak{q}_2 = ((z +: v_1) +: v_2), \\ \mathfrak{q}_3 = (((z +: v_1) +: v_2) +: v_3), \\ \ldots \\ \mathfrak{q}_n = ((((z +: v_1) +: v_2) +: v_3) \ldots +: v_n), \end{cases}$$

$$7.\quad Q = (z +: u),$$

und

$$8.\quad \begin{cases} q_1 = (z -: v_1), \\ q_2 = ((z -: v_1) -: v_2), \\ q_3 = (((z -: v_1) -: v_2) -: v_3), \\ \ldots \\ q_n = ((((z -: v_1) -: v_2) -: v_3) \ldots -\cdot v), \end{cases}$$

$$9.\quad \mathfrak{Q}_n = (z -: u),$$

so läfst sich das, was bisher von dem Lehrsatze ausgesprochen ist, in Zeichen durch die beiden Gleichungen

$$10.\quad Q = \mathfrak{q}_n \text{ und}$$
$$11.\quad \mathfrak{Q} = q_n,$$

oder auch durch die beiden Gleichungen

8*

12. $(z+:u) = ((((z+:v_1)+:v_2)+:v_3) \ldots\ldots +:v_n)$ *und*

13. $(z-:u) = ((((z-:v_1)-:v_2)-:v_3) \ldots\ldots -:v_n)$

ausdrücken.

II. *Wenn* u *in* z *aufgeht, wie in* (§. 16.), *so sind alle Reste* r, $\mathfrak{r}$, R und $\mathfrak{R}$, *Null. Hier, wo* u *in* z *nicht aufgehen soll, sind die Reste nicht Null, sondern* R *und* $\mathfrak{R}$ *werden wie folgt durch* r *und* $\mathfrak{r}$ *und durch die Factoren* v *von* u *ausgedrückt:*

14. $R = r_n v_1 v_2 v_3 \ldots\ldots v_{n-1} + r_{n-1} v_1 v_2 v_3 \ldots\ldots v_{n-2} + r_{n-2} v_1 v_2 v_3 \ldots\ldots v_{n-3} \ldots$
$\ldots + r_3 v_1 v_2 + r_2 v_1 + r_1$ *und*

15. $\mathfrak{R} = \mathfrak{r}_n v_1 v_2 v_3 \ldots\ldots v_{n-1} + \mathfrak{r}_{n-1} v_1 v_2 v_3 \ldots\ldots v_{n-2} + \mathfrak{r}_{n-2} v_1 v_2 v_3 \ldots\ldots v_{n-3} \ldots$
$\ldots + \mathfrak{r}_3 v_1 v_2 + \mathfrak{r}_2 v_1 + \mathfrak{r}_1$,

oder auch, wenn man

16. $v_1 = V_1$, $v_1 v_2 = V_2$, $v_1 v_2 v_3 = V_3 \ldots\ldots v_1 v_2 v_3 \ldots\ldots v_{n-1} = V_{n-1}$

setzt, durch

17. $R = r_n V_{n-1} + r_{n-1} V_{n-2} + r_{n-2} V_{n-3} \ldots\ldots + r_3 V_2 + r_2 V_1 + r_1$ *und*

18. $\mathfrak{R} = \mathfrak{r}_n V_{n-1} + \mathfrak{r}_{n-1} V_{n-2} + \mathfrak{r}_{n-2} V_{n-3} \ldots\ldots + \mathfrak{r}_3 V_2 + \mathfrak{r}_2 V_1 + \mathfrak{r}_1$.

III. a. *Der letzte Quotient* $\mathfrak{q}_n$ *in* (3.) *ist gleich dem letzten Quotienten* q_n *in* (2.) *wenn* u *in* z *aufgeht. Geht* u *in* z *nicht auf, so ist*

19. $\mathfrak{q}_n = q_n + 1$.

b. *Läfst man in* (3.) *die Factoren* v *und* u *in derselben Ordnung auf einander folgen, wie in* (2.), *so kann keiner der Quotienten* $\mathfrak{q}$ *gröfser sein, als der ihm correspondirende Quotient* q, *sondern nur entweder ihm gleich, oder um* 1 *kleiner.*

c. *Geht der erste Factor* v_1 *von* u *in* z *nicht auf, so sind alle Quotienten* $\mathfrak{q}$ *jeder um* 1 *gröfser, als die correspondirenden Quotienten* q.

d. *Geht der erste Factor* v_1 *von* u *in* z *auf, desgleichen der zweite Factor* v_2 *in den ersten Quotienten* q_1, *der dritte Factor* v_3 *in den zweiten Quotienten* q_2 *u. s. w. bis zum* m*ten Factor* v_m *von* u, *so sind die Quotienten* $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \ldots\ldots \mathfrak{q}_m$ *alle den Quotienten* $q_1, q_2, q_3, \ldots\ldots q_m$ *gleich; alle folgenden Quotienten* $\mathfrak{q}$ *dagegen sind sämmtlich jeder um* 1 *gröfser als die correspondirenden Quotienten* q.

Beispiel. Es sei

20. $z = 17017$ und $u = 360 = 2.2.2.3.3.5$.

a. Man nehme zuerst zu Factoren v von u folgende:

21. $v_1 = 2$, $v_2 = 2$, $v_3 = 2$, $v_4 = 3$, $v_5 = 3$, $v_6 = v_n = 5$,

so geben die Gleichungen (2. u. 3.)

$$22.\quad \begin{cases} 17017 = 8508.2+1, \\ 8508 = 4254.2+0, \\ 4254 = 2127.2+0, \\ 2127 = 709.3+0, \\ 709 = 236.3+1, \\ 236 = 47.5+1, \end{cases} \qquad 23.\quad \begin{cases} 17017 = 8509.2-1, \\ 8509 = 4255.2-1, \\ 4255 = 2128.2-1, \\ 2128 = 710.3-2, \\ 710 = 237.3-1, \\ 237 = 48.5-3. \end{cases}$$

Es ist also

$$24.\quad \begin{cases} q_1 = 8508, & q_2 = 4254, & q_3 = 2127, & q_4 = 709, & q_5 = 236, & q_6 = q_n = 47, \\ r_1 = 1, & r_2 = 0, & r_3 = 0, & r_4 = 0, & r_5 = 1, & r_6 = r_n = 1. \end{cases}$$

$$25.\quad \begin{cases} \mathfrak{q}_1 = 8509, & \mathfrak{q}_2 = 4255, & \mathfrak{q}_3 = 2128, & \mathfrak{q}_4 = 710, & \mathfrak{q}_5 = 237, & \mathfrak{q}_6 = \mathfrak{q}_n = 48, \\ \mathfrak{r}_1 = 1, & \mathfrak{r}_2 = 1, & \mathfrak{r}_3 = 1, & \mathfrak{r}_4 = 2, & \mathfrak{r}_5 = 1, & \mathfrak{r}_6 = \mathfrak{r}_n = 3; \end{cases}$$

desgleichen giebt hier (4. u. 5.)

$$26.\quad 17017 = 47.360+97 \text{ und}$$

$$27.\quad 17017 = 48.360-263,$$

also ist

$$28.\quad Q = 47, \quad R = 97,$$

$$29.\quad \mathfrak{Q} = 48, \quad \mathfrak{R} = 263.$$

Aus (24. und 28.) und aus (25. und 29.) zeigt sich, dafs, wie es nach (10. und 11.) sein soll, $Q = q_n$ $(=47)$ und $\mathfrak{Q} = \mathfrak{q}_n$ $(=48)$ ist.

Ferner ist nach (16. und 21.)

$$30.\quad V_1 = v_1 = 2,\ V_2 = v_1 v_2 = 4,\ V_3 = v_1 v_2 v_3 = 8,\ V_4 = v_1 v_2 v_3 v_4 = 24,$$
$$V_5 = v_1 v_2 \ldots v_5 = 72,\quad V_6 = v_1 v_2 \ldots v_6 = 360,$$

also geben hier (17. und 18.), gemäfs (30. 24. und 25.),

$$31.\quad R = 1.72+1.24+0.8+0.4+0.2+1 = 72+24+1 = 97 \text{ (wie 28.) und}$$

$$32.\quad \mathfrak{R} = 3.72+1.24+2.8+1.4+1.2+1$$
$$= 216+24+16+4+2+1 = 263 \text{ (wie 29.)}.$$

Desgleichen sieht man aus (24. und 25.), dafs es sich mit den q und $\mathfrak{q}$ so verhält wie es der Lehrsatz in (III. *a. b. c.*) behauptet.

b. Nimmt man zu den Factoren v von u folgende:

$$33.\quad v_1 = 12,\quad v_2 = 5,\quad v_3 = v_n = 6,$$

so geben die Gleichungen (2. und 3.)

$$34.\quad \begin{cases} 17017 = 1418.12+1, \\ 1418 = 283.\ 5+3, \\ 283 = 47.\ 6+1; \end{cases} \quad \text{und} \quad 35.\quad \begin{cases} 17017 = 1419.12-11, \\ 1419 = 284.\ 5-1, \\ 284 = 48.\ 6-4; \end{cases}$$

und es ist hier

$$36.\quad \begin{cases} q_1 = 1418, & q_2 = 283, & q_3 = q_n = 47, \\ r_1 = 1, & r_2 = 3, & r_3 = r_n = 1; \end{cases}$$

$$37.\quad \begin{cases} \mathfrak{q}_1 = 1419, & \mathfrak{q}_2 = 284, & \mathfrak{q}_3 = \mathfrak{q}_n = 48, \\ \mathfrak{r}_1 = 11, & \mathfrak{r}_2 = 1, & \mathfrak{r}_3 = \mathfrak{r}_n = 4. \end{cases}$$

Also ist zunächst wieder aus (36. und 28., 37. und 29.) $q_n = Q_n$ $(=47)$ und $\mathfrak{q}_n = \mathfrak{Q}_n$ $(=48)$.

Sodann ist hier

$$38.\quad V_1 = v_1 = 12,\quad V_2 = v_1 v_2 = 60 \quad \text{und} \quad V_3 = u = 360,$$

und (17. und 18.) geben nach (38. 37. und 36.)

$$39.\quad R = 1.60 + 3.12 + 1 = 60 + 36 + 1 = 97 \text{ (wie 28.) und}$$

$$40.\quad \mathfrak{R} = 4.60 + 1.12 + 11 = 240 + 12 + 11 = 263 \text{ (wie 29.).}$$

Alle $\mathfrak{q}$ (37.) sind wieder, gemäfs (III.), um 1 gröfser, als die correspondirenden q.

Beweis *A.* Man substituire die *zweiten* der Gleichungen (2. und 3.) in die *ersten*, so erhält man

$$41.\quad z = q_2 v_1 v_2 + r_2 v_1 + r_1 \quad \text{und}$$

$$42.\quad z = \mathfrak{q}_2 v_1 v_2 - \mathfrak{r}_2 v_1 - \mathfrak{r}_1.$$

Hierin setze man die Werthe von q_2 und $\mathfrak{q}_2$ aus den *dritten* der Gleichungen (2. und 3.), so ergiebt sich

$$43.\quad Z = q_3 v_1 v_2 v_3 + r_3 v_1 v_2 + r_2 v_1 + r_1 \quad \text{und}$$

$$44.\quad Z = \mathfrak{q}_3 v_1 v_2 v_3 - \mathfrak{r}_3 v_1 v_2 - \mathfrak{r}_2 v_1 - \mathfrak{r}_1.$$

Setzt man hierin weiter die Werthe von q_3 und $\mathfrak{q}_3$ aus den *vierten* der Gleichungen (2. und 3.), in das was sich ergiebt die Werthe von q_4 und $\mathfrak{q}_4$ aus den *fünften* der Gleichungen, und so weiter, bis zu q_n und $\mathfrak{q}_n$ aus den *letzten* der Gleichungen (2. und 3.), so erhält man

$$45.\quad Z = q_n v_1 v_2 v_3 \ldots . v_n + r_n v_1 v_2 v_3 \ldots . v_{n-1} + r_{n-1} v_1 v_2 v_3 \ldots . v_{n-2} \ldots$$
$$\ldots + r_3 v_1 v_2 + r_2 v_1 + r_1 \quad \text{und}$$

$$46.\quad Z = \mathfrak{q}_n v_1 v_2 v_3 \ldots . v_n - \mathfrak{r}_n v_1 v_2 v_3 \ldots . v_{n-1} - \mathfrak{r}_{n-1} v_1 v_2 v_3 \ldots . v_{n-2} \ldots$$
$$\ldots - \mathfrak{r}_3 v_1 v_2 - \mathfrak{r}_2 v_1 - \mathfrak{r}_1, \quad \text{oder auch}$$

$$47.\quad Z = q_n u + [r_n v_1 v_2 v_3 \ldots . v_{n-1} + r_{n-1} v_1 v_2 v_3 \ldots . v_{n-2} \ldots$$
$$\ldots + r_3 v_1 v_2 + r_2 v_1 + r_1] \quad \text{und}$$

$$48.\quad Z = \mathfrak{q}_n u - [\mathfrak{r}_n v_1 v_2 v_3 \ldots . v_{n-1} + \mathfrak{r}_{n-1} v_1 v_2 v_3 \ldots . v_{n-2} \ldots$$
$$\ldots + \mathfrak{r}_3 v_1 v_2 + \mathfrak{r}_2 v_1 + \mathfrak{r}_1].$$

B. Nun sind, wenn in (2. und 3) z. B. v_1 in z *aufgeht,* die echten Reste r_1 und $\mathfrak{r}_1$ gleich *Null* und die Quotienten q_1 und $\mathfrak{q}_1$ sind einander *gleich.* Geht auch v_2 in q_1 *auf,* so sind die Reste r_2 und $\mathfrak{r}_2$ *Null,* und auch die Quotienten q_n und $\mathfrak{q}_n$ sind einander gleich. Und so weiter

Geht dagegen v_i in z ***nicht auf,*** so sind die Reste r_1 und $\mathfrak{r}_1$ ***nicht Null;*** aber sie können auch ***nicht gröfser*** sein als v_1-1 (§. 9. II.), und der Quotient $\mathfrak{q}_1$ ist um 1 gröfser als der Quotient q_1 (§. 9. VII.). Geht v_2 in q_1 ***nicht auf,*** so sind die Reste r_2 und $\mathfrak{r}_2$ nicht Null und können ***nicht gröfser*** sein als v_2-1, und $\mathfrak{q}_2$ ist um 1 gröfser als q_2. Und so weiter.

In ***keinem*** Fall also ist $r_1>v_1-1$, $r_2>v_2-1$, $r_3>v_3-1$, ... $r_n>v_n-1$ und $\mathfrak{r}_1>v_1-1$, $\mathfrak{r}_2=v_2-1$, $\mathfrak{r}_3=v_3-1$, ... $\mathfrak{r}_n=v_n-1$. Die r und $\mathfrak{r}$ können zum Theil oder alle ***Null*** sein, aber die ***gröfsten*** Werthe, welche sie haben können, sind v_1-1, v_2-1, v_3-1, ... v_n-1.

C. Die ***kleinsten*** Werthe also Dessen, was in (47.) mit $q_n u$ durch das Pluszeichen und in (48.) mit $\mathfrak{q}_n u$ durch das Minuszeichen verbunden ist, sind ***Null,*** die ***gröfsten*** Werthe dagegen sind in (47. und 48.) ***gleichmäfsig***

49. $$(v_n-1)v_1v_2v_3\ldots v_{n-1}+(v_{n-1}-1)v_1v_2v_3\ldots v_{n-2}+(v_{n-3}-1)v_1v_2v_3\ldots v_{n-3}\ldots$$
$$\ldots+(v_3-1)v_1v_2+(v_2-1)v_1+v_1-1,$$

und Dieses thut, wenn man die angezeigten Multiplicationen ausführt,

$$v_1v_2v_3\ldots v_n+v_1v_2v_3\ldots v_{n-1}+v_1v_2v_3\ldots v_{n-2}\ldots+v_1v_2v_3+v_1v_2+v_1$$
$$-v_1v_2v_3\ldots v_{n-1}-v_1v_2v_3\ldots v_{n-2}\ldots-v_1v_2v_3-v_1v_2-v_1-1$$
$$=v_1v_2v_3\ldots v_n-1$$

50. $$=u-1.$$

Jedenfalls also sind die Summen der Glieder, die in (47. und 48.) mit $q_n u$ durch das Pluszeichen und mit $\mathfrak{q}_n u$ durch das Minuszeichen verbunden sind, ***nicht kleiner als Null*** und ***nicht gröfser als*** $u-1$.

Bezeichnet man demnach diese Summen durch s und σ, so dafs in (47. und 48.)

$$51. \quad z=q_n u+s \text{ und}$$
$$52. \quad z=\mathfrak{q}_n u-\sigma$$

ist, so ist s ein ***echter positiver*** Rest und σ ein ***echter negativer*** Rest der Division von z durch u; denn diese Reste haben jene Eigenschaft (§. 9. II.). q_n und $\mathfrak{q}_n$ sind die ***Quotienten*** der Division.

D. Dividirt man dagegen z durch u ***auf einmal*** und nimmt die ***echten positiven und negativen*** Reste, so erhält man nach (4. und 5.)

$$53. \quad z=Qu+R \text{ und}$$
$$54. \quad z=\mathfrak{Q}u-\mathfrak{R}.$$

Es giebt aber bei jeder Division ***nur einen*** echten positiven und ***nur einen*** echten negativen Rest: also mufs nothwendig

$$55. \quad R=s \text{ und } \mathfrak{R}=\sigma$$

und mithin zufolge (51. und 53.) und (52. und 54.)

$$56.\quad q_n u + R = Qu + R \quad \text{und} \quad \mathfrak{q}_n u - \mathfrak{R} = \mathfrak{Q}_n u - \mathfrak{R}$$

sein; und daraus folgt $q_n u = Qu$ und $\mathfrak{q}_n u = \mathfrak{Q}_n u$, also

$$57.\quad q_n = Q \text{ und}$$

$$58.\quad \mathfrak{q}_n = \mathfrak{Q};$$

wie es der Lehrsatz in (10. u. 11.) behauptet.

E. Aus den Werthen von s und σ in (47. u. 48.), die zufolge (55.) $= R$ und $\mathfrak{R}$ sind, folgt

$$59.\quad R = r_n v_1 v_2 v_3 \ldots . v_{n-1} + r_{n-1} v_1 v_2 v_3 \ldots . v_{n-2} + \ldots . + r_3 v_1 v_2 + r_2 v_1 + r_1$$

und

$$60.\quad \mathfrak{R} = \mathfrak{r}_n v_1 v_2 v_3 \ldots . v_{n-1} + \mathfrak{r}_{n-1} v_1 v_2 v_3 \ldots . v_{n-2} + \ldots . + \mathfrak{r}_3 v_1 v_2 + \mathfrak{r}_2 v_1 + \mathfrak{r}_1;$$

welches die Ausdrücke (14. u. 15.) des Lehrsatzes sind.

F. Da in *allen* Fällen $q_n = Q$ und $\mathfrak{q}_n = \mathfrak{Q}$ und, wenn u in z aufgeht, also R und $\mathfrak{R}$ Null sind, zufolge (4. u. 5) $Q = \mathfrak{Q}$, hingegen wenn u in z nicht aufgeht, $\mathfrak{Q} = Q + 1$ ist (§. 9. VII.), so ist auch, wenn u in z aufgeht, $q_n = \mathfrak{q}_n$, und wenn u nicht in z aufgeht, $\mathfrak{q}_n = q_n + 1$; gemäfs (19.).

G. Was für u oder V_n (16.) gilt, gilt nothwendig auch für ein Product V_m *nicht aller* v, sondern nur einer beliebigen Anzahl m der Factoren v von u. Also auch, wenn man einerseits der Reihe nach mit den in V_m enthaltenen m Factoren dividirt, was auf die Quotienten q_m und $\mathfrak{q}_m$ führt, anderseits z auf einmal durch V_m, was die Quotienten Q_m und $\mathfrak{Q}_m$ giebt, kann nur, wie in (10. u. 11.),

$$61.\quad Q_m = q_m \quad \text{und} \quad \mathfrak{Q}_m = \mathfrak{q}_m,$$

oder, wie in (III. *a.*),

$$62.\quad \mathfrak{q}_m = q_m \quad \text{oder} \quad \mathfrak{q}_m = q_m + 1$$

sein. Da nun m jede der Zahlen 1, 2, 3, ... n sein kann, und folglich q_m und $\mathfrak{q}_m$ alle die Quotienten q und $\mathfrak{q}$ in (2. und 3.) ausdrücken, so folgt, dafs kein q gröfser sein kann als das ihm correspondirende $\mathfrak{q}$, sondern nur ihm gleich, oder um 1 kleiner; wie es (III. *b.*) behauptet.

H. Geht der *erste* Factor v_1 von u, mit welchem man z dividirt, in z *nicht auf*, so ist $\mathfrak{q}_1 = q_1 + 1$ (§. 9. VII.). Aber, wenn v_1 in z nicht aufgeht, geht auch $V_m = v_1 v_2 v_3 \ldots . v_m$, für eine beliebige Zahl m von Factoren v, in z nicht auf (§. 15. I.). Also ist für die Quotienten $\mathfrak{Q}_m$ und Q_m der Division von z durch V_m, $\mathfrak{Q}_m = Q_m + 1$ (§. 9. VII.). Es ist aber *immer* $\mathfrak{q}_m = \mathfrak{Q}_m$ und $q_m = Q_m$ (61.), also ist auch nothwendig

$$63.\quad \mathfrak{q}_m = q_m + 1.$$

Hieraus folgt, da m jede der Zahlen 1, 2, 3, ... n sein kann, dafs, wenn der *erste* Factor v_1 von u in z nicht aufgeht, *alle* Quotienten $\mathfrak{q}$ jeder um 1 gröfser sind als die correspondirenden Quotienten q. Dies behauptet (III. *c.*).

I. Geht $V_m = v_1 v_2 v_3 \dots v_m$ in z auf, so gehen, nach (§. 15. II.), auch alle die Factoren $V_{m-1} = v_1 v_2 v_3 \dots v_{m-1}$, $V_{m-2} = v_1 v_2 v_3 \dots v_{m-2}$, ... $V_2 = v_1 v_2$ und $V_1 = v_1$ von V_m in z auf. Also sind alle die Quotienten Q_m, Q_{m-1}, Q_{m-2}, ... Q_1 den Quotienten $\mathfrak{Q}_m$, $\mathfrak{Q}_{m-1}$, $\mathfrak{Q}_{m-2}$, ... $\mathfrak{Q}_1$ der Reihe nach gleich; und da Q *immer* gleich q und $\mathfrak{Q}$ *immer* gleich $\mathfrak{q}$ ist, so sind auch die Quotienten q_m, q_{m-1}, ... q_1 der Reihe nach den Quotienten $\mathfrak{q}_m$, $\mathfrak{q}_{m-1}$, ... $\mathfrak{q}_1$ gleich.

Der hier vorausgesetzte Fall, dafs $V_m = v_1 v_2 v_3 \dots v_m$ in z *aufgeht*, ist aber *der*, wenn zuerst v_1 in z aufgeht, darauf v_2 in den Quotienten $q_1 = \frac{z}{v_1}$, v_3 in den Quotienten $q_2 = \frac{q_1}{v_2}$ u. s. w.: denn z enthält alsdann nothwendig alle die Factoren $v_1, v_2, v_3, \dots v_m$, also $\frac{z}{v_1} = q_1$ noch die Factoren $v_2, v_3, \dots v_m$, $\frac{q_1}{v_2} = q_2$ noch die Factoren $v_3, v_4, \dots v_m$ u. s. w. Also, wenn v_1 in z aufgeht, v_2 in $q_1 = \frac{z}{v_1}$, v_3 in $q_2 = \frac{q_1}{v_2}$, und so weiter bis zu q_m, so sind alle die Quotienten $q_1, q_2, q_3, \dots q_m$ der Reihe nach den Quotienten $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \dots$ ... $\mathfrak{q}_m$ *gleich.*

Geht $V_{m+1} = v_1 v_2 v_3 \dots v_m v_{m+1}$ nicht mehr in z auf, so gehen, gemäfs (§. 15. I.), auch V_{m+2}, V_{m+3}, ... V_n nicht in z auf, und dann gilt für die mit V_{m+1}, V_{m+2}, ... V_n correspondirenden Quotienten q_{m+1}, q_{m+2}, ... q_n und $\mathfrak{q}_{m+1}$, $\mathfrak{q}_{m+2}$, ... $\mathfrak{q}_n$ wieder das, was sich in (*H.*) fand, nemlich, dafs alle $\mathfrak{q}$ um 1 gröfser sind, als die correspondirenden q.

Dieses zusammengenommen ist, was (III. *d.*) behauptet.

Anm. Der Beweis von (I. u. II.) des Lehrsatzes, von (*A.* bis *F.*), beruht insbesondere auf dem Umstande, dafs, wie es die Rechnung mit Hülfe von (§. 9) ergiebt, die Summen der in (47. u. 48.) mit $q_n u$ und $\mathfrak{q}_n u$ durch $+$ und $-$ verbundenen Glieder nicht kleiner als Null und nicht gröfser als $u-1$ sein können. Der Beweis von (III.) des Lehrsatzes, von (*G.* bis *I.*), nimmt (§. 9. u. 15) zu Hülfe und beruht nächstdem darauf, dafs das, was für $u = V_n$ gilt, auch für V_m gelten mufs; wo m jede Zahl von 1 bis n sein kann.

§. 18.

Lehrsatz.

Wenn z_1, z_2, z_3, ... z_n beliebige positive oder negative ganze Zahlen sind, und es ist

$$1. \quad z_1 \pm z_2 \pm z_3 \ldots\ldots \pm z_{n-1} = z_n,$$

oder auch, da die z sowohl positiv als negativ sollen sein können,

$$2. \quad z_1 \pm z_2 \pm z_3 \ldots\ldots z_{n-1} \pm z_n = 0,$$

so geht jede ganze Zahl, welche Gemeintheiler aller z bis auf eines ist, auch noch in dieses eine auf und ist folglich ein Gemeintheiler aller.

Beweis. Einer der Gemeintheiler z. B. von z_1, z_2, z_3, ... z_{n-1} sei die ganze Zahl u und es sei

$$3. \quad \frac{z_1}{u} = w_1, \quad \frac{z_2}{u} = w_2, \quad \frac{z_3}{u} = w_3, \quad \ldots\ldots \quad \frac{z_{n-1}}{u} = w_{n-1}, \quad \frac{z_n}{u} = w_n,$$

so sind *nach der Voraussetzung* w_1, w_2, w_3, ... w_{n-1} sämmtlich *ganze* Zahlen.

Dividirt man nun die Gleichung (1.) mit u, so ergiebt sich

$$4. \quad \frac{z_1}{u} \pm \frac{z_2}{u} \pm \frac{z_3}{u} \ldots\ldots \pm \frac{z_{n-1}}{u} = \frac{z_n}{u},$$

also, wenn (3.) in (1.) substituirt wird,

$$5. \quad w_1 \pm w_2 \pm w_3 \ldots\ldots \pm w_{n-1} = w_n = \frac{z_n}{u}.$$

Aber w_1, w_2, w_3, ... w_{n-1} sind sämmtlich *ganze* Zahlen, und die Verbindung ganzer positiver oder negativer Zahlen durch Zusammenzählen ist ebenfalls eine ganze Zahl. Also ist vermöge (5.) nothwendig auch $w_n = \frac{z_n}{u}$ eine *ganze* Zahl, und folglich geht nothwendig der Gemeintheiler u aller z, bis auf das eine z_n, auch in dieses eine auf (§ 14. III.), und ist folglich ein Gemeintheiler *aller* z.

§. 19.

Lehrsatz.

Von zwei beliebigen theilbaren oder untheilbaren, ungleichen ganzen Zahlen sei z_1 die grössere, z_2 die kleinere. Man dividire z_1 durch z_2 und nehme den echten positiven oder negativen Rest r, dessen Werth zeichenfrei also $< z_2$ ist, oder auch den unbedingt echten oder

den kleinsten Rest. Hierauf dividire man die kleinere Zahl z_2 durch den Rest r_1 und nehme wieder beliebig den echten positiven oder negativen oder den kleinsten Rest r_2, dessen Werth zeichenfrei also $< r_1$ ist. Man dividire r_1 durch r_2 auf gleiche Weise und nehme den Rest r_3, der $< r_2$ ist. Man dividire r_2 durch r_3 auf gleiche Weise und nehme den Rest r_4, der $< r_3$ ist. Fährt man so immer weiter fort, so ergiebt sich Folgendes.

I. *Zuletzt kommt man immer nothwendig auf einen Rest r_n, welcher Null ist.*

II. *Der vorletzte Rest r_{n-1} ist immer der gröfste Gemeintheiler von z_1 und z_2, so wie von z_2 und r_1, und von allen auf einander folgenden Paaren von Resten; desgleichen von der Gesammtheit der Zahlen $z_1, z_2, r_1, r_2, r_3, \ldots r_{n-1}$, nicht aber nothwendig von zweien oder mehreren unter ihnen, die nicht unmittelbar auf einander folgen. Diese können auch gröfsere Gemeintheiler haben.*

III. *Ist der vorletzte Rest r_{n-1} gleich 1, so sind die zwei Zahlen z_1 und z_2, desgleichen z_2 und der erste Rest r_1, so wie auch alle je zwei auf einander folgenden Reste nothwendig theilerfremd; desgleichen ist dann die Gesammtheit der Zahlen $z_1, z_2, r_1, r_2, \ldots r_{n-1}$ gemeintheilerfremd; nicht aber sind nothwendig zwei oder mehrere dieser Zahlen, die nicht unmittelbar auf einander folgen, theilerfremd.*

IV. *Sind umgekehrt die beiden Zahlen z_1 und z_2 theilerfremd, so ist der vorletzte Rest r_{n-1} nothwendig gleich 1; und auch z_2 und der erste Rest r_1, sammt allen Paaren auf einander folgender Reste, jedoch nicht nothwendig die nicht unmittelbar auf einander folgenden, sind theilerfremd. Gemeintheilerfremd aber ist die Gesammtheit der Zahlen $z_1, z_2, r_1, r_2, \ldots r_{n-1}$.*

V. *Sind die beiden Zahlen z_1 und z_2 theilerverwandt, und man dividirt sie, so wie alle Reste r, mit ihrem gröfsten Gemeintheiler, der nach (II.) der vorletzte Rest r_{n-1} ist, welcher in sie allein aufgeht, so gilt von den Quotienten derselben, was in dem Falle (IV.) von den Zahlen $z_1, z_2, r_1, r_2, \ldots r_{n-1}$ selbst gilt.*

Beweis I. *A.* Die verschiedenen in dem Satz beschriebenen Divisionen werden durch

$$1. \quad \begin{cases} z_1 = \mathfrak{S} z_2 \pm r_1, \\ z_2 = \mathfrak{S} r_1 \pm r_2, \\ r_1 = \mathfrak{S} r_2 \pm r_3, \\ r_2 = \mathfrak{S} r_3 \pm r_4, \\ \dots\dots\dots\dots \\ r_{n-4} = \mathfrak{S} r_{n-3} \pm r_{n-2}, \\ r_{n-3} = \mathfrak{S} r_{n-2} \pm r_{n-1}, \\ r_{n-2} = \mathfrak{S} r_{n-1} \pm r_n \end{cases}$$

ausgedrückt, wo die r die *zeichenfreien Zahlenwerthe* der *Reste* bezeichnen, für welche dann nach Belieben die Zeichen $+$ oder $-$ gelten können.

B. Die *zeichenfreien* Zahlenwerthe, welche die r ausdrücken, sind, selbst dann, wenn man nicht die *unbedingt echten* Reste nimmt, jedenfalls *kleiner* als die zugehörigen Divisoren, da die r jedenfalls *echte* Reste sein sollen; das heifst: es ist, den *zeichenfreien* Zahlenwerthen nach,

$$2. \quad r_1 < z_2, \quad r_2 < r_1, \quad r_3 < r_2, \quad r_4 < r_3, \quad \dots\dots$$

C. Die zeichenfreien Zahlenwerthe von r_1, r_2, r_3, ... nehmen daher nothwendig *immer fort ab;* keiner kann *gröfser* als der vorhergehende, oder auch nur ihm *gleich* sein, sondern *nur kleiner;* also wenigstens um 1. Daraus folgt, dafs man zuletzt nothwendig auf einen Rest r_n kommen mufs, der *Null* ist. Denn wie klein auch schon der zeichenfreie Zahlenwerth eines r sein mag: es kann, wenn dieser Werth noch nicht Null sein sollte, durch fortgesetzte Division ein *noch kleineres* r hervorgebracht werden; so lange, bis die Grenze 0 der Kleinheit erreicht ist. Dieses ist was (I.) behauptet.

Beweis von II. *D.* Da zufolge (I.) der letzte Rest r_n *immer* nothwendig Null ist, so reducirt sich die *letzte* der Gleichungen (1.) *immer* auf

$$3. \quad r_{n-2} = \mathfrak{S} r_{n-1},$$

welches ausdrückt, dafs r_{n-2} ein *Vielfaches* von r_{n-1}, nemlich das $\mathfrak{S}$*fache* von r_{n-1} ist und dafs also r_{n-1} in r_{n-2} *aufgeht.* Also ist r_{n-1} ein *Gemeintheiler* von r_{n-1} und r_{n-2}, und zwar der *gröfste* Gemeintheiler, da in r_{n-1} keine *gröfsere* Zahl aufgehen kann, als *sie selbst.*

E. Hieraus folgt, vermöge der *vorletzten* Gleichung in (1.) und vermöge (§. 18.), dafs r_{n-1} auch in r_{n-3} aufgehen mufs. Denn da es in den beiden ganzen Zahlen r_{n-1} und r_{n-2} aufgeht, so mufs es vermöge jener vorletzten Gleichung

$$4. \quad r_{n-3} = \mathfrak{S} r_{n-2} + r_{n-1}$$

zufolge (§. 18.) auch in die ganze Zahl r_{n-3} aufgehen. Also ist r_{n-1} auch

ein ***Gemeintheiler*** von r_{n-2} und r_{n-3}, und zwar der ***gröfste;*** denn hätten r_{n-3} und r_{n-2} einen gröfsern Gemeintheiler als r_{n-1}, so müfste derselbe, vermöge ***derselben*** Gleichung (4.) zufolge (§. 18.) auch in r_{n-1} aufgehen; was nicht möglich ist, da keine Zahl in eine ***kleinere*** aufgeht.

F. Daraus, dafs r_{n-1} der ***gröfste Gemeintheiler*** von r_{n-3} und r_{n-2} ist, folgt weiter, vermöge der vorvorletzten Gleichung (1.), nemlich aus

$$6. \quad r_{n-4} = \mathfrak{S}\, r_{n-3} + r_{n-2}$$

und aus (§. 18.), dafs r_{n-1} auch in r_{n-4} aufgehen und also, eben so wie von r_{n-2} und r_{n-3}, auch von r_{n-3} und r_{n-4} ein ***Gemeintheiler*** sein mufs, und zwar wiederum der ***gröfste;*** denn hätte r_{n-3} und r_{n-4} einen gröfseren Gemeintheiler als r_{n-1}, so müfste derselbe vermöge der nemlichen Gleichung (6.) und (§. 18.) auch in r_{n-2} aufgehen; also hätten r_{n-3} und r_{n-2} einen gröfsern Gemeintheiler als r_{n-1}; was nach (*E.*) nicht der Fall ist.

G. Auf ganz gleiche Weise folgt aus den weiter vorhergehenden Gleichungen in (1.), dafs r_{n-1} auch der ***gröfste Gemeintheiler*** von r_{n-4} und r_{n-5}, von r_{n-5} und r_{n-6} u. s. w. und zuletzt von r_1 und r_2 ist. Sodann folgt aus der zweiten der Gleichungen (1.), und immer aus gleichen Gründen, dafs r_{n-1} auch der gröfste Gemeintheiler von z_2 und r_1 ist, und aus der ***ersten*** der Gleichungen (1.), dafs r_{n-1} nicht minder der ***gröfste Gemeintheiler*** von z_1 und z_2 ist.

Der ***vorletzte Rest*** r_{n-1} ist also *immer,* unter allen Umständen, der ***gröfste Gemeintheiler*** von z_1 und z_2, so wie von z_2 und r_1, von r_1 und r_2 von r_2 und r_3, und überhaupt von jedem Paare ***unmittelbar aufeinander folgender*** Reste.

H. Daraus folgt ferner, dafs r_{n-1} in ***allen*** den Zahlen z_1, z_2, r_1, r_2, ... r_{n-1} ***zugleich*** aufgeht, und dafs es also *ein* ***Gemeintheiler*** derselben, und zwar der ***gröfste*** ist, da in der ***letzten*** dieser Zahlen r_{n-1} keine gröfsere Zahl aufgehen kann, als sie selbst.

Es kann aber allerdings *gröfsere* Theiler als r_{n-1} geben, die in zwei oder mehrere ***nicht*** unmittelbar auf einander folgende Reste aufgehen. Denn wenn es auch keinen gröfsern Theiler als r_{n-1} giebt, der z. B. in r_2 und r_3 zugleich aufgeht, so kann es doch einen gröfsern Gemeintheiler von r_2 und $\mathfrak{S}$*mal* r_3 geben, welcher, der Gleichung $r_2 = \mathfrak{S} r_3 + r_4$ gemäfs, zugleich in r_4 aufgeht u. s. w.

Dieses zusammen ist was (II.) behauptet.

Beweis von III. *I.* Da nach (II.) der vorletzte Rest r_{n-1} der *gröfste* Gemeintheiler von z_1 und z_2, von z_2 und r_1, von r_1 und r_2 und weiter von allen Paaren unmittelbar auf einander folgender Reste ist, so folgt, dafs, in dem Fall wenn $r_{n-1} = 1$ ist, alle die genannten Zahlenpaare mit *keiner gröfsern* Zahl als 1 aufgehen und mithin *theilerfremd* sind. Auch hat jetzt die Gesammtheit der Zahlen z_1, z_2, r_1, r_2, ... r_{n-1} keinen gröfsern *Gemeintheiler* als 1, und ist folglich *gemeintheilerfremd.* Nicht aber sind nothwendig nicht unmittelbar auf einander folgende von jenen Zahlen theilerfremd; aus demselben Grunde wie in (*H.*). Dieses ist was (III.) behauptet.

Beweis von IV. *K.* Sind z_1 und z_2 *theilerfremd,* so sind es vermöge der ersten Gleichung in (1.) auch z_2 und r_1; denn hätten z_2 und r_1 einen gröfsern Gemeintheiler als 1, so müfste derselbe zufolge (§. 18.) auch in z_1 *aufgehen,* und folglich hätten dann z_2 und z_1 einen gröfsern Gemeintheiler als 1; der Voraussetzung entgegen.

L. Daraus, dafs hier z_2 und r_1 nothwendig theilerfremd sind, folgt weiter, vermöge der *zweiten* der Gleichungen (2.), ganz auf dieselbe Weise wie in (*K.*), dafs auch nothwendig r_1 und r_2 theilerfremd sind. Hieraus folgt, vermöge der *dritten* Gleichung (1.), wieder auf dieselbe Weise, dafs auch r_2 und r_3 theilerfremd sind; und so weiter fort, bis zu r_{n-2} und r_{n-1}.

M. Es folgt also zunächst, dafs, wenn z_1 und z_2 theilerfremd sind, das Gleiche auch mit allen den Zahlenpaaren z_2 und r_1, r_1 und r_2, r_2 und r_3 bis zu r_{n-2} und r_{n-1} der Fall ist.

N. Nun ist aber, was auch r_{n-1} sein mag, nach (II.) r_{n-1} *immer* der *gröfste* Gemeintheiler von z_1 und z_2: in dem gegenwärtigen Falle, wo z_1 und z_2 *theilerfremd* sein sollen, *haben* sie keinen gröfsern Gemeintheiler als 1: also ist in diesem Fall auch nothwendig $r_{n-1} = 1$.

Dieses behauptet der Lehrsatz in (IV.). Das Übrige von (IV.) folgt ähnlich wie für (III.).

Beweis von V. *O.* Dividirt man z_1 und z_2 mit ihrem *gröfsten* Gemeintheiler r_{n-1}, der zufolge (II.) zugleich der gröfste Gemeintheiler aller der Zahlenpaare z_2 und r_1, r_1 und r_2, r_2 und r_3 bis zu r_{n-2} und r_{n-1} ist und folglich in sie alle aufgeht, so haben alle die Zahlen nun *keinen* Gemeintheiler mehr; folglich sind alle die *Quotienten* paarweise theilerfremd, und mithin in demselben Falle, wie wenn z_1 und z_2 theilerfremd wären. Also gilt von diesen Quotienten Dasselbe, was in dem Falle (IV.) von den Zahlen z_1, z_2, r_1, r_2, ... r_{n-1} selbst gilt. Dieses behauptet (V.).

Anm. 1. Die Beweise der verschiedenen Theile des Lehrsatzes beruhen insbesondere darauf, dafs, wenn *zwei* Zahlen in einer Gleichung mit *drei Gliedern* einen Theiler gemein haben, derselbe nach (§. 18.) auch in die *dritte* Zahl aufgehen mufs.

Anm. 2. Wenn man den *gröfsten Gemeintheiler* r_{n-1} zweier gegebenen Zahlen z_1 und z_2 nach dem Lehrsatze *ausrechnen* will, so wird man wohl thun, nicht sowohl immer die *echten positiven*, oder immer die *echten negativen* Reste zu nehmen, sondern vielmehr *immer* die *unbedingt echten* oder *kleinsten* Reste. Denn da von jenen nach (§. 9. II.) die zeichenfreien Zahlenwerthe nur nothwendig kleiner als der *ganze Divisor*, von den *unbedingt echten* Resten dagegen die zeichenfreien Zahlenwerthe nach (§. 9. IV.) nothwendig kleiner als die *Hälfte des Divisors* sind, so werden die Reste der verschiedenen Divisionen, wenn man die *kleinsten* Reste nimmt, schneller abnehmen und man wird also damit eher zum Ziele gelangen.

Es sei z. B. $z_1 = 9012$ und $z_2 = 6459$, so ist die Rechnung nach den drei verschiedenen Arten folgende:

$$7.\quad \left\{\begin{array}{rcl} 9012 &=& 1.6459 + 2553 \\ 6459 &=& 2.2553 + 1353 \\ 2553 &=& 1.1353 + 1200 \\ 1353 &=& 1.1200 + 153 \\ 1200 &=& 7.\ 153 + 129 \\ 153 &=& 1.\ 129 + 24 \\ 129 &=& 5.\ 24 + 9 \\ 24 &=& 2.\ 9 + 6 \\ 9 &=& 1.\ 6 + 3 \\ 6 &=& 2.\ 3 + 0 \end{array}\right.$$

$$8.\quad \left\{\begin{array}{rcl} 9012 &=& 2.6459 - 3906 \\ 6459 &=& 2.3906 - 1353 \\ 3906 &=& 3.1353 - 153 \\ 1353 &=& 9.\ 153 - 24 \\ 153 &=& 7.\ 24 - 15 \\ 24 &=& 2.\ 15 - 6 \\ 15 &=& 3.\ 6 - 3 \\ 6 &=& 2.\ 3 - 0 \end{array}\right.$$

$$9.\quad \left\{\begin{array}{rcl} 9012 &=& 1.6459 + 2553 \\ 6459 &=& 3.2553 - 1200 \\ 2553 &=& 2.1200 + 153 \\ 1200 &=& 8.\ 153 - 24 \\ 153 &=& 6.\ 24 + 9 \\ 24 &=& 3.\ 9 - 3 \\ 9 &=& 3.\ 3 + 0 \end{array}\right.$$

In (7.) sind durchweg die *positiven echten* Reste, in (8.) die *negativen echten* Reste und in (9.) die *unbedingt echten* Reste genommen. Die letzte

Rechnung ist, wie sich zeigt, die kürzeste. Der ***gröfste Gemeintheiler*** von z_1 und z_2 und von *allen* Resten $r_1, r_2, r_3, \ldots r_{n-1}$, so wie aller ***Paare unmittelbar*** auf einander folgender Reste ist hier $r_{n-1} = 3$. Aber 3 ist nicht der *gröfste* Gemeintheiler ***nicht unmittelbar*** auf einander folgender Reste. Z. B. die beiden Reste 1200 und 24 in (7. und 9.) haben nicht blofs 3 sondern 24 zum *gröfsten* Gemeintheiler.

§. 20.

Lehrsatz.

I. ***Wenn eine ganze Zahl*** u ***zu jeder der beiden beliebigen ganzen Zahlen*** z_1, z_2 ***theilerfremd ist, so ist sie es auch zu ihrem Producte*** $z_1 z_2$; ***gleichviel ob*** z_1 ***und*** z_2 ***ungleich oder einander gleich, theilerverwandt oder theilerfremd sind.***

II. ***Wenn eine untheilbare oder Stammzahl*** p ***in keine der beiden ganzen Zahlen*** z_1 ***und*** z_2 ***aufgeht, so geht sie auch in ihr Product*** $z_1 z_2$ ***nicht auf, gleichviel, wie vorhin, was*** z_1 ***und*** z_2 ***sein mögen.***

Beispiele. *No. 1.* Die Zahl $u = 8$ ist zu jeder der Zahlen $z_1 = 15$ und $z_2 = 21$ theilerfremd: zu dem Product $z_1 z_2 = 15.21 = 315$ ist sie es gleichfalls.

No. 2. Die untheilbare Zahl 11 geht in keine der beiden Zahlen $z_1 = 24$ und $z_2 = 81$ auf; und in ihr Product $z_1 z_2 = 24.81 = 1944$ ebenfalls nicht.

Beweis von I. *A.* Die Zahl u kann weder *gleich* z_1 noch *gleich* z_2 sein, denn sonst wäre sie zu z_1 oder zu z_2 nicht *theilerfremd.* Sie kann also nur *kleiner* oder *gröfser* sein, als die eine oder die andere der beiden Zahlen z_1 und z_2, z. B. als z_1.

B. Je nachdem u *kleiner* oder *gröfser* ist als z_1, setze man:

$$1.\ \begin{cases} z_1 = \mathfrak{G} u \pm r_1, \\ u = \mathfrak{G} r_1 \pm r_2, \\ r_1 = \mathfrak{G} r_2 \pm r_3, \\ r_2 = \mathfrak{G} r_3 \pm r_4, \\ \ldots\ldots\ldots\ldots \\ r_{n-4} = \mathfrak{G} r_{n-3} \pm r_{n-2}, \\ r_{n-3} = \mathfrak{G} r_{n-2} \pm r_{n-1}, \\ r_{n-2} = \mathfrak{G} r_{n-1} \pm r_n; \end{cases} \quad \text{oder} \quad 2.\ \begin{cases} u = \mathfrak{G} z_1 \pm \varrho_1, \\ z_1 = \mathfrak{G} \varrho_1 \pm \varrho_2, \\ \varrho_1 = \mathfrak{G} \varrho_2 \pm \varrho_3, \\ \varrho_2 = \mathfrak{G} \varrho_3 \pm \varrho_4, \\ \ldots\ldots\ldots\ldots \\ \varrho_{n-4} = \mathfrak{G} \varrho_{n-3} \pm \varrho_{n-2}, \\ \varrho_{n-3} = \mathfrak{G} \varrho_{n-2} \pm \varrho_{n-1}, \\ \varrho_{n-2} = \mathfrak{G} \varrho_{n-1} \pm \varrho_n; \end{cases}$$

wo die r und die ϱ sämmtlich entweder ***positive,*** oder ***negative,*** oder ***unbedingt echte*** Reste bezeichnen, jedenfalls aber ***echte Reste.***

C. Zufolge (§. 19. I. und IV.) ist hier nothwendig, da z_1 und u theilerfremd vorausgesetzt werden, nächst

$$3.\quad r_n = 0 \quad \text{und} \quad \varrho_n = 0, \text{ auch}$$

$$4.\quad r_{n-1} = \pm 1 \quad \text{und} \quad \varrho_{n-1} = \pm 1,$$

so dafs sich die ***beiden letzten*** Gleichungen in (1. u. 2.) auf

$$5.\ \begin{cases} r_{n-3} = \mathfrak{G} r_{n-2} \pm 1, \\ r_{n-2} = \mathfrak{G}.1 \end{cases} \quad \text{und} \quad 6.\ \begin{cases} \varrho_{n-3} = \mathfrak{G} \varrho_{n-2} \pm 1, \\ \varrho_{n-2} = \mathfrak{G}.1 \end{cases}$$

reduciren.

D. Nun multiplicire man die sämmtlichen Gleichungen (1. und 2.), zugleich auf (5. und 6.) Rücksicht nehmend, mit z_2, so erhält man

$$7.\ \begin{cases} z_1 z_2 = \mathfrak{G} u z_2 \pm r_1 z_2, \\ u z_2 = \mathfrak{G} r_1 z_2 \pm r_2 z_2, \\ r_1 z_2 = \mathfrak{G} r_2 z_2 \pm r_3 z_2, \\ r_2 z_2 = \mathfrak{G} r_3 z_2 \pm r_4 z_2, \\ \dots\dots\dots\dots \\ r_{n-4} z_2 = \mathfrak{G} r_{n-3} z_2 \pm r_{n-2} z_2, \\ r_{n-3} z_2 = \mathfrak{G} r_{n-2} z_2 \pm z_2 \\ r_{n-2} z_2 = \mathfrak{G} z_2; \end{cases} \qquad 8.\ \begin{cases} u z_2 = \mathfrak{G} z_1 z_2 \pm \varrho_1 z_2, \\ z_1 z_2 = \mathfrak{G} \varrho_1 z_2 \pm \varrho_2 z_2, \\ \varrho_1 z_2 = \mathfrak{G} \varrho_2 z_2 \pm \varrho_3 z_2, \\ \varrho_2 z_2 = \mathfrak{G} \varrho_3 z_2 \pm \varrho_4 z_2, \\ \dots\dots\dots\dots \\ \varrho_{n-4} z_2 = \mathfrak{G} \varrho_{n-3} z_2 \pm \varrho_{n-2} z_2, \\ \varrho_{n-3} z_2 = \mathfrak{G} \varrho_{n-2} z_2 \pm z_2, \\ \varrho_{n-2} z_2 = \mathfrak{G} z_2. \end{cases}$$

E. Hätten nun in dem Falle $z_1 > u$, auf welchen sich die Gleichungen (7.) beziehen, u und das ***Product*** $z_1 z_2$ einen ***Gemeintheiler*** $\lambda > 1$, so müfste derselbe vermöge der *ersten* der Gleichungen (7.), nach (§. 18.), auch in $r_1 z_2$ ***aufgehen,*** also in $u z_2$ und $r_1 z_2$ ***zugleich,*** mithin vermöge der ***zweiten*** Gleichung (7.), nach (§. 18.), auch in $r_2 z_2$, folglich in $r_1 z_2$ und $r_2 z_2$ ***zugleich,*** folglich auch vermöge der *dritten* Gleichung (7.), nach (§. 18.), auch in $r_3 z_2$, und so weiter; folglich zuletzt vermöge der *vorletzten* der Gleichungen (7.) auch in z_2, mithin in u und z_2 ***zugleich,*** was der Voraussetzung entgegen ist, also kann ein Gemeintheiler von u und $z_1 z_2$, z. B. λ, ***nicht*** gröfser sein als 1.

F. Hätten in dem Falle $z_1 < u$, auf welchen sich die Gleichungen (8.) beziehen, u und das ***Product*** $z_1 z_2$ einen ***Gemeintheiler*** $z > 1$, so müfste derselbe vermöge der *ersten* der Gleichungen (8.), nach (§. 18), auch in $\varrho_1 z_2$ ***aufgehen,*** also in $z_1 z_2$ und $\varrho_1 z_2$ ***zugleich,*** mithin vermöge der ***zweiten*** Gleichung (8.), nach (§. 18.), auch in $\varrho_2 z_2$ und folglich in $\varrho_1 z_2$ und $\varrho_2 z_2$ ***zu-***

gleich, folglich auch vermöge der *dritten* Gleichung (8.), nach (§. 18.), in $\varrho_3 z_2$, und so weiter; folglich zuletzt vermöge der vorletzten der Gleichungen (8.) auch in z_2, und mithin in u und z_2 *zugleich;* was wieder der Voraussetzung entgegen ist, so dafs auch hier ein Gemeintheiler λ von u und $z_1 z_2$ nicht gröfser als 1 sein kann.

G. Es können also in *keinem* Fall u und das Product $z_1 z_2$ einen Theiler $\lambda > 1$ gemein haben, insofern u und z_2 einen solchen Gemeintheiler *nicht* haben oder *theilerfremd* sind. Dafs u und z_1 *theilerfremd* sind ist in (*C.*) bedungen worden, weil ohne das nicht nothwendig die vorletzten Reste r_{n-1} und ϱ_{n-1} gleich 1 sein und folglich von den Gleichungen (7. und 8.) die vorletzten nicht Statt finden würden. Also folgt, dafs *u, in der Voraussetzung,* es sei sowohl zu z_1 als zu z_2 *theilerfremd,* auch nothwendig zu dem Product $z_1 z_2$ von z_1 und z_2 *theilerfremd* sein mufs.

Beweis von II. *H.* Eine *untheilbare* Zahl p hat keinen andern Theiler > 1 als *sich selbst.* Sie ist daher zu z_1 und z_2 *immer* theilerfremd, wenn sie nicht etwa selbst in z_1 oder z_2 *aufgeht.* Also folgt aus (I.), dafs die untheilbare Zahl p, wenn sie nicht selbst in z_1 oder in z_2 aufgeht, auch in das Product $z_1 z_2$ von z_1 und z_2 nicht aufgehen kann; wie es (II.) behauptet.

I. Übrigens ändert sich an dem Beweise offenbar nichts, es mögen z_1 und z_2 einander gleich oder ungleich, zu einander theilerverwandt oder theilerfremd sein; dem Lehrsatz gemäfs.

Anm. Der Beweis beruht zunächst auf dem Umstande, dafs zufolge (§. 19.) die Gleichungen (4.) *nur dann* nothwendig Statt finden, wenn u und z_1 und z_2 theilerfremd sind; aufserdem auf dem Lehrsatz (§. 18.).

(Die Fortsetzung folgt.)

2.

Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré à quatre indéterminées.

(Par Mr. G. *Eisenstein* à Berlin.)

Je veux énoncer dans cette note un théorème fort singulier sur les formes *cubiques* qui établit une liaison très remarquable entre la théorie de ces formes et celle de la *multiplication* des formes *quadratiques.*

Je nomme forme cubique toute expression telle que

$$1.\quad ax^3+3bx^2y+3cxy^2+dy^3,$$

où a, b, c, d sont des nombres entiers donnés et x, y des indéterminées. En formant l'ensemble de toutes les expressions semblables dans lesquelles cette forme se change par l'application de toutes les substitutions de la forme

$$2.\quad x = \alpha x'+\beta y',\quad y = \gamma x'+\delta y'$$

les entiers α, β, γ, δ étant tels que

$$3\quad \alpha\delta-\beta\gamma = 1,$$

nous aurons ce que je nomme *classe* de formes *cubiques* équivalentes, ou *classe cubique.*

Chaque forme cubique a pour correspondante une forme quadratique

$$4.\quad Ax^2+2Bxy+Cy^2 = F = (A, B, C)$$

dont les coëfficients sont liés avec ceux de la forme cubique par les équations très simples

$$5.\quad A = b^2-ac,\quad 2B = bc-ad,\quad C = c^2-bd,$$

et si l'on applique tant à la forme cubique qu'à la forme quadratique une substitution quelconque (2.), la même liaison existera entre les coëfficients des deux nouvelles formes que l'on obtiendra par cette double transformation, ensorte qu'à une classe entière de formes *cubiques* correspondra toujours une classe complète de formes *quadratiques,* et que toutes les *classes cubiques* se distribueront sur diverses *classes quadratiques:* propriété remarquable qui jette un nouveau jour sur la nature des formes cubiques.

Comme ces préliminaires suffiront pour me faire comprendre, voici le théorème qui suit.

„Soit D un déterminant quelconque, mais ***sans diviseur carré.*** Distinguons parmi les classes du genre principal ceux qui, par leur ***triplication*** produisent la ***classe principale;*** je dis que pour ces classes il existera toujours une classe cubique qui leur correspondra, et que pour chacune d'elles il n'en existera qu'une seule, tandis qu'aucune classe cubique ne correspondra au reste des classes quadratiques, ni dans le genre principal, ni dans tous les autres genres."

Il en est différemment si le déterminant a un diviseur carré.

La théorie générale de la distribution des classes cubiques sur les classes quadratiques dépend de la considération des classes qui en général produisent par leur triplication une classe quadratique quelconque donnée K de l'ordre primitif, mais laquelle peut être produite par la triplication. On pourrait désigner ces classes par le symbole $\sqrt[3]{K}$; alors si le déterminant est régulier, ce symbole aura une signification réelle et une seule signification pour chaque classe K, quand le nombre total des classes (proprement primitives) n'est pas divisible par *trois;* *) mais quand ce nombre est un multiple de *trois,* il y aura un tiers parmi les classes K pour lequel l'expression $\sqrt[3]{K}$ a une valeur réelle et *triple,* tandis que pour les autres classes le symbole $\sqrt[3]{K}$ n'a point de signification réelle.

Le théorème précédent est intimément lié avec la proposition suivante.

La lettre D ayant la même signification comme ci-dessus, l'équation indéterminée à quatre variables:

$$6.\quad x_1^2 x_4^2 - 3x_2^2 x_3^2 + 4x_1 x_3^3 + 4x_4 x_2^3 - 6x_1 x_2 x_3 x_4 = 4D$$

a la propriété, qu'on peut déduire par une formule générale une infinité de solutions d'une seule formule que l'on suppose connue. En effet, soit donnée une solution de cette équation par le système:

$$7.\quad \xi_1,\ \xi_2,\ \xi_3,\ \xi_4,$$

on aura généralement

$$8.\quad \begin{cases} x_1 = \alpha^3\xi + 3\alpha^2\gamma\xi_2 + 3\alpha\gamma^2\xi_3 + \gamma^3\xi_4, \\ x_2 = \alpha^2\beta\xi_1 + (\alpha^2\delta + 2\alpha\beta\gamma)\xi_2 + (2\alpha\gamma\delta + \beta\gamma^2)\xi_3 + \gamma^2\delta\xi_4, \\ x_3 = \alpha\beta^2\xi_1 + (\beta^2\gamma + 2\alpha\beta\delta)\xi_2 + (2\beta\gamma\delta + \alpha\delta^2)\xi_3 + \gamma\delta^2\xi_4, \\ x_4 = \beta^3\xi_1 + 3\beta^2\delta\xi_2 + 3\beta\delta^2\xi_3 + \delta^3\xi_4, \end{cases}$$

*) Mr. *Lejeune Dirichlet* a désigné le premier ce nombre remarquable par un procédé fort ingénieux. Voyez „Recherches sur diverses applications etc. Vol. 19 et 21 de ce journal."

les entiers α, β, γ étant tels que

$$9. \quad \alpha\delta - \beta\gamma = 1.$$

De cette manière la *totalité* des solutions de l'équation proposée pourra toujours être distribuée dans un nombre de groupes distincts, en comprenant dans un même groupe deux solutions qui se déduisent l'une de l'autre par les équations (8.). Le nombre de ces groupes est exactement celui qui désigne le nombre des classes quadratiques pour le déterminant D qui, par leur triplication produisent la classe principale, nombre qui pour un déterminant régulier est ou *trois* ou *l'unité*, selon que le nombre total des classes est ou n'est pas divisible par *trois*, mais qui peut être assez considérable pour un déterminant irrégulier.

Voici encore un autre théorème sur expression des nombres par des formes cubiques que j'ai tiré de la même source, et qui n'est pas moins élégant.

„Soit

$$10. \quad ax^3 + 3bx^2y + 3cxy^2 + dy^3 = f$$

une forme cubique donnée, pour laquelle $bc - ad$ est un nombre *pair*; soit de plus

$$b^2 - ac = A, \quad bc - ad = 2B, \quad c^2 - bd = C, \quad B^2 - AC = D.$$

Cela posé, si nous désignons par

$$11. \quad N, \quad N', \quad N'', \quad N''', \text{ etc.}$$

la série de tous les nombres différents et premiers avec $2D$ qui peuvent être représentés par la forme quadratique

$$12. \quad (A, B, C) = Ax^2 + 2Bxy + Cy^2,$$

de manière que les valeurs des indéterminées soient premières entre elles: je dis que tous les *nombres premiers à* $2D$, *exprimables par la forme cubique* f et par des valeurs des indéterminées premières entre elles, seront donnés par les *valeurs* de V qui se trouvent parmi les solutions des équations suivantes:

$$13. \quad U^2 - DV^2 = N^3, \quad U^2 - DV^2 = N'^3, \text{ etc. etc.}$$

U et V étant des nombres premiers entre eux."

On verra par cet abrégé, que la nouvelle théorie, dont je viens de donner quelques résultats est succeptible à beaucoup de développements, et quelle se recommande à l'attention des géomètres.

Peut être communiquerai je plus tard la théorie complète que j'ai formée de cette partie tout-à-fait nouvelle de la théorie des nombres.

Je profite de cette occasion pour donner quelques formules nouvelles sur les fonctions elliptiques, mais qui ne sont que des cas bien particuliers d'une équation très-générale. Les voici. On a

$$1+\frac{x}{R}+\frac{x^2}{R^4}+\frac{x^3}{R^9}+\dots+\frac{x^n}{R^{n^2}}+\text{ in inf.}$$

$$=\cfrac{1}{1-\cfrac{x}{R-\cfrac{(1-R^2)x}{R^3-\cfrac{x}{R^3-\cfrac{(1-R^4)x}{R^4-\cfrac{x}{R^5-\cfrac{(1-R^6)x}{R^6-\text{etc. in inf.}}}}}}}}$$

Soit m un nombre impair et ϱ une racine primitive de l'équation

$$Z^m = 1,$$

on aura

$$1+\varrho x+\varrho^4 x^2+\varrho^9 x^3+\dots+\varrho^{(m-1)^2}x^{m-1}$$

$$=\cfrac{1-x^m}{1-\cfrac{x}{\varrho^{m-1}-\cfrac{(1-\varrho^{m-2})x}{\varrho^{m-2}-\text{etc.}}}}\,,\qquad \text{fraction continue et } \textit{finie.}$$

$$\ddots\;\cfrac{}{\varrho^2-\cfrac{(1-\varrho)x}{\varrho-\cfrac{x}{1-\cfrac{(1-\varrho^{m-1})x}{\varrho^{m-1}-\text{etc.}}}}}$$

$$\ddots\;\cfrac{}{\varrho^3-\cfrac{(1-\varrho^2)x}{\varrho^2-\cfrac{x}{\varrho}}}$$

En posant

$$K=\int_0^{\frac{1}{2}\pi}\frac{d\varphi}{\sqrt{(1-k^2\sin^2\varphi)}},\qquad K'=\int_0^{\frac{1}{2}\pi}\frac{d\varphi}{\sqrt{(1-k'^2\sin^2\varphi)}},$$

$$k^2+k'^2=1,\qquad p=e^{\pi\frac{K'}{K}},$$

on aura

$$\frac{2K}{\pi} = \left(1 + \cfrac{2}{p - \cfrac{1}{p^2 - \cfrac{1-p^2}{p^3 - \cfrac{1}{p^4 - \cfrac{1-p^4}{p^5 - \cfrac{1}{p^6 - \text{in inf.}}}}}}}\right)^2$$

$$= 1 + \cfrac{4p}{1+p^2 - \cfrac{p(1+p^2)^2}{1+p^4 + \cfrac{p^3(1-p^2)^2}{1+p^6 - \cfrac{p^3(1+p^4)^2}{1+p^8 + \cfrac{p^5(1-p^4)^2}{1+p^{10} - \text{etc.}}}}}}$$

Je n'entre pas dans d'autres détails sur ces résultats, en espérant que j'aurai l'occasion d'offrir aux géomètres la théorie entière assez étendue qui alors contiendra leur démonstration.

Berlin en Décembre 1843.

4.

Über die Anzahl der quadratischen Formen, welche in der Theorie der complexen Zahlen zu einer reellen Determinante gehören.

(Von Hrn. G. *Eisenstein*, Stud. zu Berlin.)

Der berühmte Verfasser des Beweises über die unbegrenzte arithmetische Progression ist durch seine vortrefflichen Untersuchungen über die Anzahl der quadratischen Formen in der gewöhnlichen reellen Theorie sowohl, als in der Theorie der complexen Zahlen von der Form $a+b\sqrt{-1}$, neben der vollständigen Lösung des Problems selbst, auch noch auf die Entdeckung eines Satzes geführt worden, welcher ohne Zweifel wegen seiner Einfachheit und Eleganz zu den schönsten Wahrheiten der höhern Arithmetik gerechnet werden kann.

Dieser grofse Zahlentheoretiker findet nämlich, dafs „die Anzahl der quadratischen Formen für eine reelle Determinante D in der Theorie der aus vierten Wurzeln der Einheit zusammengesetzten complexen Zahlen gleich ist dem Product der beiden Anzahlen quadratischer Formen in der reellen Theorie für die beiden Determinanten $+D$ und $-D$, wenn die unbestimmte Gleichung $t^2-Du^2=-1$ in ganzen reellen Zahlen lösbar ist; oder aber gleich der Hälfte jenes Productes im entgegengesetzten Falle."

Da ich einen analogen Satz in der Theorie der aus *dritten* Wurzeln der Einheit zusammengesetzten Zahlen vermuthete, so stellte ich die entsprechende Untersuchung für diese complexen Zahlen an und wurde zu dem folgenden Resultate geführt.

„In der Theorie der aus *dritten* Wurzeln der Einheit zusammengesetzten Zahlen ist die Formen-Anzahl für eine reelle Determinante D immer gleich dem halben Producte der Formen-Anzahlen für die beiden Determinanten D und $-3D$ in der reellen Theorie."

Berlin im December 1843.

5.

Allgemeine Auflösung der Gleichungen von den ersten vier Graden.

(Von Hrn. Stud. *G. Eisenstein* zu Berlin.)

Bei der Auflösung der höhern Gleichungen begnügte man sich gewöhnlich, wie es scheint, mit dem Nachweis ihrer Möglichkeit, indem man sich von der wirklichen Darstellung der Endresultate durch die grofse Weitläufigkeit der Rechnung abschrecken liefs. Ich gebe hier diese Endresultate für die ersten vier Grade vollständig entwickelt; und zwar nehme ich die Gleichungen ganz allgemein an, da jede Beschränkung der Coëfficienten, wie z. B., dafs der erste Coëfficient der Einheit, oder dafs der zweite der Null gleich sein soll, nur eine Beeinträchtigung der Eleganz und des wahren Characters der Resultate herbeiführt.

I. Die Gleichung vom ersten Grade $ax+b=0$ giebt $x=-\frac{b}{a}$.

II. Für die Auflösung der Gleichungen vom 2ten, 3ten und 4ten Grade mufs man zwei neue Functionen $\varphi(\lambda)$ und $\psi(\lambda)$ einführen, die respective durch die Gleichungen $\varphi^2=\lambda$, $\psi^3=\lambda$ bestimmt werden. Die Function $\varphi(\lambda)$ hat für jedes λ zwei Werthe $\pm\varphi(\lambda)$, während die andere $\psi(\lambda)$ drei Werthe annimmt, die sich durch einen derselben auf folgende Weise ausdrücken lassen:

$$\psi(\lambda),\quad \varrho\psi(\lambda),\quad \varrho^2\psi(\lambda),$$

wo ϱ den Ausdruck $\frac{1}{2}(-1+\varphi(-3))$ vorstellt.

Bezeichnet man nun noch der Kürze halber durch A, B, C, D, E, F die nachstehenden homogenen ganzen Functionen:

$$A = b^2-ac,$$
$$B = 3abc-a^2d-2b^3,$$
$$C = a^2d^2-3b^2c^2+4ac^3+4db^3-6abcd,$$
$$D = ae+3c^2-4bd,$$
$$E = ad^2+b^2e-ace-2bcd+c^3,$$
$$F = 27a^2d^4+27b^4e^2+18a^2c^2e^2-36b^2c^2d^2-54a^2cd^2e-54ab^2ce^2$$
$$-108abcd^3-108b^3cde+6ab^2d^2e+54ac^3d^2+54b^2c^3e+180abc^2de$$
$$-81ac^4e-a^3e^3+64b^3d^3+12a^2bde^2,$$

so sind die Wurzeln der allgemeinen quadratischen Gleichung

$$ax^2+2bx+c=0:$$

$$x=\frac{1}{a}[-b\pm\varphi(A)].$$

III. Für die allgemeine cubische Gleichung

$$ax^3+3bx^2+3cx+d=0$$

findet sich

$$x=\begin{cases}\frac{1}{a}[-b+\ \psi(\alpha)+\ \psi(\beta)],\\ \frac{1}{a}[-b+\varrho\psi(\alpha)+\varrho^2\psi(\beta)],\\ \frac{1}{a}[-b+\varrho^2\psi(\alpha)+\varrho\psi(\beta)];\end{cases}$$

wo

$$\alpha=\tfrac{1}{2}(B+a\varphi(C)),\qquad \beta=\tfrac{1}{2}(B-a\varphi(C))$$

und wo die zusammengehörigen Werthe der beiden Functionen $\psi(\alpha)$ und $\psi(\beta)$ vollkommen bestimmt werden durch die Gleichung

$$\psi(\alpha)\psi(\beta)=A=b^2-ac.$$

IV. Die allgemeine biquadratische Gleichung

$$ax^4+4bx^3+6cx^2+4dx+e=0$$

giebt

$$x=\begin{cases}\frac{1}{a}[-b+\varphi(\gamma)+\varphi(\delta)+\varphi(\varepsilon)],\\ \frac{1}{a}[-b+\varphi(\gamma)-\varphi(\delta)-\varphi(\varepsilon)],\\ \frac{1}{a}[-b-\varphi(\gamma)+\varphi(\delta)-\varphi(\varepsilon)],\\ \frac{1}{a}[-b-\varphi(\gamma)-\varphi(\delta)+\varphi(\varepsilon)];\end{cases}$$

wo

$$\left.\begin{aligned}\gamma&=A+\tfrac{1}{3}a[\psi(\zeta)+\psi(\eta)],\\ \delta&=A+\tfrac{1}{3}a[\varrho\psi(\zeta)+\varrho^2\psi(\eta)],\\ \varepsilon&=A+\tfrac{1}{3}a[\varrho^2\psi(\zeta)+\varrho\psi(\eta)],\end{aligned}\right\}\quad \begin{aligned}\zeta&=\frac{9E+\varphi(3F)}{9},\\ \eta&=\frac{9E-\varphi(3F)}{9}.\end{aligned}$$

Zur Bestimmung der zusammengehörigen Werthe dienen die beiden Gleichungen

$$\psi(\zeta)\psi(\eta)=\tfrac{1}{3}D,\quad \text{und}\quad \varphi(\gamma)\varphi(\delta)\varphi(\varepsilon)=\tfrac{1}{4}B.$$

Die Wurzeln der allgemeinen Gleichung vom 5ten Grade nehmen eine ganz ähnliche Form an, wenn man aufser den Functionen $\varphi(\lambda)$ und $\psi(\lambda)$ noch eine dritte neue Function $\chi(\lambda)$ einführt, die durch die Gleichung



$$\chi^5+\chi = \lambda \text{ *)}$$

gegeben ist. Auf die sehr merkwürdigen Eigenschaften und Umformungen der homogenen Ausdrücke, welche in die Auflösungsformeln der algebraischen Gleichungen eingehen, werde ich bei einer andern Gelegenheit zurückkommen; wo man auch ihren Nutzen in der Zahlentheorie wahrnehmen wird.

Berlin, am 1. Januar 1844.

---

*) $\chi(\lambda) = \lambda - \lambda^5 + 10\frac{\lambda^9}{2!} - 15.14\frac{\lambda^{13}}{3!} + 20.19.18\frac{\lambda^{17}}{4!} - \text{in inf.}$
$= \sqrt[5]{(\lambda - \sqrt[5]{(\lambda - \text{in inf.}))}}$.

6.

Resultate der Auflösung von drei geometrischen Aufgaben; für Liebhaber des algebraischen Calculs.

(Von Herrn Prof. Dr. *Lehmus* zu Berlin.)

---

1. Aufgabe. Im Coordinatenraume XOY ist ein Punct B durch seine Coordinaten $OA = a$ auf OX und $AB = b$, parallel mit OY, gegeben: die Lage der Geraden durch B zu bestimmen, welche zwischen ihren Durchschnittspuncten D, E mit den Richtungen der Achsen OX, OY die bestimmte Länge $DE = c$ haben.

Wird AD durch x ausgedrückt, so wird für $x = \sqrt[3]{(ab^2)}$, $DE = [a^{\frac{2}{3}} + b^{\frac{2}{3}}]^{\frac{3}{2}} = h$ ein Minimum für c im ersten rechtwinkligen Coordinatenraum $X\Theta Y$, und für diesen Werth h von c finden sich noch zwei Werthe von x, nämlich

$$x = -a - \sqrt[3]{(ab^2)} \pm \sqrt{(a^2 + (abh)^{\frac{2}{3}})},$$

für welche beide $c = h$ in den anliegenden Coordinatenräumen liegt. Die Aufgabe liefert also drei Resultate, wenn $c = h$ ist.

Für alle übrigen Werthe von c, kleiner oder gröſser als h, bestimmen sich die Werthe für x aus der Formel

$$x = \tfrac{1}{2}\left[-a - \alpha \pm \sqrt{\left(3(a^2 - 2d^2) - \alpha^2 + \frac{2a(b^2 + c^2)}{\alpha}\right)}\right],$$

wenn $\frac{1}{3}(a^2 + b^2 + c^2)$ durch d^2, abc durch p^3, $p^3 + \sqrt{(p^6 + d^6)}$ durch P^3 ausgedrückt und, erstlich, wenn $c < h$ ist,

$$\alpha = +\sqrt{\left(a^2 - 2d^2 + P^2 + \frac{d^4}{P^2}\right)}$$

genommen wird, so daſs in allen diesen Fällen jedesmal nur zwei Resultate entstehen, für welche c in die beiden anliegenden Coordinatenräume fällt. Ist aber, zweitens, $c > h$, so ist

$$\alpha = \pm\sqrt{(a^2 - 4d^2 . \cos^2 \tfrac{1}{3}(2n\pi + \varphi))}$$

zu nehmen, wenn $n = -1$ oder $= 0$, oder $= +1$ gesetzt und unter φ der Winkel verstanden wird, für welchen

$$\cos\varphi = -\frac{2p^6 + d^6}{d^6}$$

ist, so daſs in allen diesen Fällen jedesmal vier Lagen für c eintreten: zwei im ersten Coordinatenraum, und in jedem der beiden anliegenden Coordinatenräume eine.

2. Aufgabe. In einem gegebenen Dreieck die Lage des Punctes A zu bestimmen, für welchen die drei Normalen aus A auf die drei Seiten das Dreieck in drei gleiche Theile theilen.

Bezeichnen α, β, γ die drei Winkel des Dreiecks; wird die α gegenüberliegende Seite zur Längen-Einheit genommen, die Winkelspitze zu β zum Anfangspunct O der Coordinaten; bezeichnen x, y die Coordinaten des gesuchten Punctes A; wird $\beta-\gamma$ durch δ, $2+\cos^2\beta$ durch a, $2+\cos^2\gamma$ durch b ausgedrückt und dann w aus der Gleichung

$$w^3-3[ab-(2+\cos^2\alpha)\sin^2\delta]\,w+(a+b)[ab-2\sin^2\alpha\sin^2\delta+9\sin^2\delta]-81\sin^2\delta=0,$$

ferner P aus der Gleichung $P^2\sin^2\alpha=\frac{1}{3}(w+a+b)$; dann B und C aus den Formeln

$$B=\tfrac{1}{2}\left[P^2-\frac{a+b}{6\sin^2\alpha}+\frac{\sin\delta}{3P\sin^3\alpha}\right],\quad C=\tfrac{1}{2}\left[P^2-\frac{a+b}{6\sin^2\alpha}-\frac{\sin\delta}{3P\sin^3\alpha}\right];$$

und dann die Werthe von z aus den Gleichungen

$$z^2+Pz+B=0 \quad\text{und}\quad z^2-Pz+C=0$$

entnommen, so hat man

$$x=z+\tfrac{1}{2} \quad\text{und}\quad y=\frac{\sin\delta\cot\alpha+3\cos\beta\cos\gamma-6x\cos\beta\cos\gamma}{6[x\sin\alpha-\cos\beta\sin\gamma]},$$

und nur diejenigen der sich ergebenden Werthe können der Aufgabe entsprechen, für welche A innerhalb des Dreiecks oder in eine der drei Seiten fällt.

Ist $\beta=\gamma$, so genügt $w=1$, $P=\operatorname{cosec}\alpha\sqrt{\tfrac{1}{3}}$, $B=C=0$, $z=0$, $x=\frac{1}{2}$ und $y=\frac{1}{2}[\operatorname{tang}\beta-\sec\beta.\sqrt{\tfrac{1}{3}}]$; welche Werthe auch aus einer besonderen unmittelbaren Lösung der Aufgabe viel einfacher hervorgehen.

3. Aufgabe. Aus den drei Transversalen a, b, c, welche die Winkel 2α, 2β, 2γ eines Dreiecks halbiren, diese Winkel unter der Voraussetzung zu finden, dafs $b=c$, also auch $\beta=\gamma$ sei.

Es ergiebt sich, wenn n die Werthe -1, 0 und 1, und φ den Winkel ausdrückt, für welchen $\cos\varphi=\frac{8a^3-27ab^2}{[4a^2+9b^2]^{\frac{3}{2}}}$ ist:

$$\sin\beta=\frac{1}{3b}\left[a+\sqrt{(4a^2+9b^2)}.\cos\tfrac{1}{3}(2n\pi+\varphi)\right].$$

Ist $a:b=1:2$, so geht aus der ursprünglichen Bedingungsgleichung sogleich $5\beta=90^\circ$, also $\beta=18^\circ$ hervor, und die Richtigkeit dieses Resultats ist leicht synthetisch nachzuweisen. Die Vermuthung, dafs die Lösung der allgemeinen Aufgabe, wenn auch b und c verschieden sind, auf symmetrische Formen führen müsse, wie die Lösung der ähnlichen Aufgabe: „Aus den drei Transversalen, welche auf den gegenüberliegenden Seiten normal stehen, oder dieselben halbiren etc." zeigt sich durch die für den besonderen Fall erhaltene Formel als richtig.

7.

Aufgaben.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

---

1. Wenn n und k zwei beliebig gegebene ganze Zahlen sind und $k<n$ ist, so kann man die Summe der Reihe

$$\frac{x^k}{k!}+\frac{x^{k+n}}{(k+n)!}+\frac{x^{k+2n}}{(k+2n)!}+\text{etc. in inf.}=\varphi(n,k,x)$$

immer durch Exponentialfunctionen ausdrücken. Bezeichnet man nämlich durch ϱ eine primitive Wurzel der Gleichung

$$z^n=1,$$

so findet sich

$$\varphi=\frac{1}{n}[e^x+\varrho^{-k}e^{\varrho x}+\varrho^{-2k}e^{\varrho^2 x}+\ldots.+\varrho^{-(n-1)k}e^{\varrho^{n-1}x}].$$

Man verlangt nun alle reellen und imaginären Werthe von x, d. h. alle Werthe von der Form $\alpha+\beta\sqrt{-1}$, für welche die Function φ verschwindet. Für den Fall $n=2$ ist die Aufgabe schon gelöset.

2. Durch Hülfe der *Gaufs*schen Formeln kann man ebenfalls die Summe der Reihe

$$\sum_{s=1}^{s=\infty}\left(\frac{s}{D}\right)\frac{x^s}{s!}=\psi$$

in Kreisfunctionen ausdrücken, wenn man nämlich unter D eine gegebene ganze Zahl und unter $\left(\frac{s}{D}\right)$ das bekannte *Legendre*sche Zeichen, oder die Null versteht, wenn s mit D einen gemeinschaftlichen Theiler hat. Man sucht alle Werthe von x, welche $\psi=0$ machen.

3. Welche Bedingungen müssen erfüllt werden, damit die beiden complementären elliptischen Quadranten

$$K=\int_0^{\frac{1}{2}\pi}\frac{d\varphi}{\sqrt{(1-k^2\sin^2\varphi)}},\qquad K'=\int_0^{\frac{1}{2}\pi}\frac{d\varphi}{\sqrt{(1-k'^2\sin^2\varphi)}},$$

für welche $k^2+k'^2=1$ ist, ein rationales Verhältnifs zu einander haben? Dieser Fall tritt z. B. bei der Lemniscata ein, für welche $k=k'=\sqrt{(\frac{1}{2})}$, also $K=K'$ ist.

4. Wenn D eine positive ganze Zahl von der Form $8n+5$ ist: welches Criterium läfst sich angeben, um a priori zu entscheiden, ob die

Gleichung $p^2 - Dq^2 = 4$ in *ungeraden* Zahlen p und q lösbar ist, oder nicht, oder, was auf dasselbe hinauskommt, ob die Anzahl der *uneigentlich* primitiven Classen quadratischer Formen für die Determinante D das Einfache oder das Dreifache beträgt von der Anzahl der *eigentlich* primitiven Classen für dieselbe Determinante?

5. Es ist bekannt die Summe der Reihe

$$\Sigma^k A_k x^k = \varphi(x),$$

wo sich das Summenzeichen über eine gewisse endliche oder unendliche Anzahl von Werthen der ganzen Zahl k erstreckt: wie läfst sich die Summe der folgenden Reihe finden

$$\psi = \Sigma \varrho^{\text{Ind.}\,k} A_k x^k \text{ (k relative Primzahl zu p)},$$

in welcher Ind. k diejenige Zahl μ bezeichnet, welche für eine gegebene Primzahl p und eine zu dieser gehörige gegebene primitive Congruenzwurzel g der Congruenz $g^\mu \equiv k \pmod{p}$ genügt, und wo ferner ϱ irgend eine Wurzel der Gleichung $z^p = 1$ vorstellt?

6. Zu beweisen, dafs es unendlich viele Primzahlen von der Form $2^{2^n} + 1$ giebt.

7. Wie kann man für eine gegebene ganze Zahl p die Reihe interpoliren, deren allgemeines Glied $\left(\frac{n}{p}\right)$ ist?

8. Ein Criterium anzugeben, um zu erkennen, ob die Anzahl der Classen eigentlich primitiver quadratischer Formen für die Determinante D durch 3 theilbar sei, oder nicht; und wenn der erste Fall stattfindet, diejenigen Classen anzugeben, welche fähig sind, durch die Triplication anderer Classen erzeugt zu werden.

9. Es sei D eine regelmäfsige Determinante, für welche jedes Genus eine doppelzahlige Form (forma ambigua) enthält; n sei die Anzahl der eigentlich primitiven Classen für diese Determinante, und μ eine beliebige ungerade Zahl. Dann sind zwei Fälle möglich: entweder ist μ ein Theiler von n, oder nicht. Im zweiten Falle hat jede Classe die Eigenschaft, dafs sie durch μfaches Zusammensetzen einer andern Classe mit sich selbst, und zwar nur aus einer einzigen, auf diese Art entstehen kann. Ist dagegen μ ein Theiler von n, so giebt es nur $\frac{n}{\mu}$ Classen, welche die Eigenschaft haben, durch Vervielfältigung anderer Classen entstehen zu können. Diese $\frac{n}{\mu}$ Classen, deren jede aus μ verschiedenen Classen durch μfaches Zusammensetzen entstehen kann, und zu

denen immer die Fundamentalclasse mitgehört, zeichnen sich also hierdurch vor allen übrigen Classen aus, und ein näheres Eingehen auf ihre speciellen Eigenschaften und Beziehungen möchte vielleicht zu nicht uninteressanten Resultaten führen. Namentlich scheinen auch diejenigen Classen Aufmerksamkeit zu verdienen, welche durch μfaches Zusammensetzen mit sich selbst die Fundamentalclasse erzeugen, und welche einige Analogie mit den μten Wurzeln der Einheit haben.

10. Wenn a und b zwei gegebene *rationale* Ausdrücke vorstellen: die Bedingungen anzugeben, unter welchen zwei andere *rationale* Ausdrücke α und β gefunden werden können, so dafs

$$\sqrt[3]{(a+\sqrt{(b)})} = \alpha+\beta\sqrt{(b)}$$

ist. *Rational* heifse im Allgemeinen jeder Ausdruck von der Form $p+q\sqrt{-1}$, für welchen p und q reell und zugleich rational sind.

11. *Gaufs* hat in seiner Kreistheilung gezeigt, dafs für jede Primzahl n das Polynom

$$4(x^{n-1}+x^{n-2}+\ldots\ldots+x+1) = 4X$$

auf die Form

$$Y^2+(-1)^{\frac{1}{2}(n-1)}Z^2,$$

gebracht werden kann, wo Y und Z ganze Functionen von x sind. Es fragt sich, ob diese Zerlegung *nur auf eine* Weise, oder ob sie auf mehrere Arten und auf wie viele Arten sie gemacht werden könne. Für $n=3$ giebt z. B. die Kreistheilung $4(x^2+x+1)=(2x+1)^2+3$; es ist aber noch aufserdem $4(x^2+x+1)=(x-1)^2+3(x+1)^2$. Die Beantwortung dieser Frage ist von Wichtigkeit für den Beweis des *Fermat*schen Satzes, von welchem *Euler* und *Lejeune Dirichlet* specielle Fälle behandelt haben.

Berlin, im December 1843.

Crelle, Journal d. Math. Bd. XXVII Heft 1.

Facsimile einer Handschrift von Kepler.

Clarissime D. Praeceptor Dudum ultro citroq. com me
at nuderint, inveni locum aliquem in Cardano, qui
rem nostram automatariam mirifice illustrat. Sic
„ igr ille lib: 16, de Subtilitate. Nuper etiam
„ quidam illam machinam mundi universalem, olim a
„ Gulielmo Zelandino fabricatam, atq. dissolutam in tene-
„ bris per incuriam marcescentem, cum ego, quodam
„ bono fato, ad instaurandum bonas artes, etiam obiter, non
„ minus quam ex industria, natus, in lucem revocassem,
„ in integrum restituit.

8.

Untersuchungen über die cubischen Formen mit zwei Variabeln.

(Von Herrn Stud. *Gotth. Eisenstein* zu Berlin.)

Erste Abtheilung.

§. 1.

Jeder Ausdruck von der Form

$$1.\quad ax^3+3bx^2y+3cxy^2+dy^3 = (a, b, c, d) = f,$$

in welchem a, b, c, d gegebene, x, y unbestimmte ganze Zahlen vorstellen, heifst eine *cubische Form*.

Bezeichnet man die Coëfficientenverbindungen

$$2.\quad b^2-ac,\quad bc-ad,\quad c^2-bd$$

respective durch

$$A,\qquad B,\qquad C,$$

so heifst die quadratische Form

$$3.\quad Ax^2+Bxy+Cy^2 = F$$

die *determinirende Form* der cubischen Form f. Endlich nenne ich die Determinante der quadratischen Form $2F$, nämlich

$$4.\quad B^2-4AC = D\,^{*}),$$

die *Determinante* der cubischen Form f. Diese Determinante kann auf folgende Art in die Coëfficienten der cubischen Form ausgedrückt werden:

$$5.\quad D = (bc-ad)^2-4(b^2-ac)(c^2-bd)$$
$$= a^2d^2-3b^2c^2+4ac^3+4db^3-6abcd.$$

Die Determinante D ist genau diejenige Verbindung, von deren Vorzeichen es abhängt, ob die Gleichung

$$ax^3+3bx^2+3cx+d = 0$$

nur eine oder drei reelle Wurzeln hat.

Wird ω der gröfste gemeinschaftliche Theiler von a, b, c, d genannt, ω_1 der von $a, 3b, 3c, d$ und Ω der von A, B, C, so ist ω^2, wie man aus den Gleichungen (2.) sieht, immer ein Theiler von Ω, während Ω^2 und

*) Nach *Gaufs* ist D die Determinante der Form $2F = 2Ax^2+2Bxy+2Cy^2$.

ω^4 wiederum Theiler von D sind. So oft also D keinen biquadratischen Theiler hat, können auch a, b, c, d keinen gemeinschaftlichen Theiler haben.

§. 2.

Wendet man auf die cubische Form

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

die Substitution

$$6.\quad x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y' \quad \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$$

an, und ordnet das Resultat nach den neuen Variabeln x' und y', so erhält man die neue cubische Form

$$f' = a'x'^3 + 3b'x'^2y' + 3c'x'y'^2 + d'y'^3,$$

deren Coëfficienten a', b', c', d' auf folgende Art durch die alten Coëfficienten a, b, c, d ausgedrückt werden können:

$$7.\quad \begin{cases} a' = a\alpha^3 + 3b\alpha^2\gamma + 3c\alpha\gamma^2 + d\gamma^3, \\ b' = a\alpha^2\beta + b(\alpha^2\delta + 2\alpha\beta\gamma) + c(2\alpha\gamma\delta + \beta\gamma^2) + d\gamma^2\delta, \\ c' = a\alpha\beta^2 + b(\beta^2\gamma + 2\alpha\beta\delta) + c(2\beta\gamma\delta + \alpha\delta^2) + d\gamma\delta^2, \\ d' = a\beta^3 + 3b\beta^2\delta + 3c\beta\delta^2 + d\delta^3. \end{cases}$$

Die Form f' heifst unter der Form f enthalten, weil jede durch f' darstellbare Zahl auch durch f darstellbar ist; aber nicht umgekehrt.

Die Transformation $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ heifst eine eigentliche oder uneigentliche Transformation, je nachdem $\alpha\delta - \beta\gamma$, welches durch ε bezeichnet sein mag, positiv oder negativ ist.

Die Gleichungen (6.),

$$\alpha x' + \beta y' = x \quad \text{und} \quad \gamma x' + \delta y' = y,$$

nach x und y aufgelöset, geben

$$x' = \frac{\delta x - \beta y}{\varepsilon}, \quad y' = \frac{-\gamma x + \delta y}{\varepsilon}.$$

Ist daher

$$7.\quad \alpha\delta - \beta\gamma = \varepsilon = \pm 1,$$

so hat man zugleich eine Transformation von f' in f, nämlich die folgende:

$$\begin{pmatrix}\delta, & -\beta\\ -\beta, & \alpha\end{pmatrix}.$$

In diesem Falle enthalten also die beiden Formen f und f' einander gegenseitig und heifsen aequivalente cubische Formen; und zwar wird ihre Aequivalenz eine eigentliche oder uneigentliche genannt, je nachdem

$$\alpha\delta - \beta\gamma = +1, \quad \text{oder} \quad \alpha\delta - \beta\gamma = -1 \text{ ist.}$$

Es ist nun leicht, foldende Sätze zu beweisen:

„Wenn die Form f die Form f', und f' die f'' enthält, so enthält auch die f die f''."

„Wenn f und f', so wie f' und f'' aequivalente Formen sind, so sind auch f und f'' aequivalent" u. s. w.

Diese Sätze und ihre Beweise sind durchaus analog den entsprechenden für die quadratischen Formen; ich halte mich deshalb nicht bei denselben auf, da es mir nur besonders darauf ankomint, das den cubischen Formen Eigenthümliche und Characteristische hervorzuheben.

„Sind f und f' aequivalent, welches ich so bezeichne:

$$f \backsim f',$$

so sind sowohl die ω als die ω_1 für beide dieselben." Dies ergiebt sich aus dem blofsen Anblick der Gleichungen (7.) und der ihnen entsprechenden beim Übergange von f' zu f.

Eine cubische Form bildet mit der Gesammtheit aller ihr aequivalenter cubischer Formen eine *Classe* cubischer Formen.

Für jede Classe aequivalenter cubischer Formen haben ω und ω_1 einen ganz bestimmten Werth.

§. 3.

Lehrsatz. „Enthält eine cubische Form f eine zweite f', und geht sie durch die Transformation $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ in f' über, so enthält auch die determinirende Form F der cubischen Form f, die determinirende Form F' der Form f', und zwar geht F durch die Transformation

$$\begin{pmatrix}\alpha\varepsilon, & \beta\varepsilon\\ \gamma\varepsilon, & \delta\varepsilon\end{pmatrix}$$

in F' über; und sind die beiden cubischen Formen aequivalent, so sind es auch die determinirenden Formen; und zwar gehen die letzteren durch dieselbe Transformation in einander über; wie die ersteren."

Beweis. Wenn man die Coëfficienten der determinirenden Form F', nämlich

$$b'^2 - a'c', \quad b'c' - a'd', \quad c'^2 - b'd'$$

vermittels der Gleichungen (7.) in die Coëfficienten der cubischen Form f, nämlich a, b, c, d ausdrückt, so findet man, nach den nöthigen Reductionen,

$$b'^2 - a'c' = \varepsilon^2[(b^2 - ac)\alpha^2 + (bc - ad)\alpha\gamma + (c^2 - bd)\gamma^2],$$
$$b'c' - a'd' = \varepsilon^2[2(b^2 - ac)\alpha\beta + (bc - ad)(\alpha\delta + \beta\gamma) + 2(c^2 - bd)\gamma\delta],$$
$$c'^2 - b'd' = \varepsilon^2[(b^2 - ac)\beta^2 + (bc - ad)\beta\delta + (c^2 - bd)\delta^2].$$

Diese Gleichungen lassen sich, wenn A', B', C' die Coëfficienten von F vorstellen, folgendermaafsen schreiben:

$$9.\quad \begin{cases} A' = A(\alpha\varepsilon)^2 + B\,\alpha\varepsilon.\gamma\varepsilon + C(\gamma\varepsilon)^2, \\ B' = 2A\,\alpha\varepsilon.\beta\varepsilon + B(\alpha\varepsilon.\delta\varepsilon + \beta\varepsilon.\gamma\varepsilon) + 2C\,\gamma\varepsilon.\delta\varepsilon, \\ C' = A(\beta\varepsilon)^2 + B\,\beta\varepsilon.\delta\varepsilon + C(\delta\varepsilon)^2. \end{cases}$$

Dieselben Gleichungen findet man aber merkwürdigerweise ebenfalls, wenn man auf die Form

$$F = Ax^2 + Bxy + Cy^3$$

die Substitution

$$10.\quad x = \alpha\varepsilon.x' + \beta\varepsilon.y', \qquad y = \gamma\varepsilon.x' + \delta\varepsilon.y', \qquad \text{d. h.}\ \begin{pmatrix}\alpha\varepsilon, & \beta\varepsilon \\ \gamma\varepsilon, & \delta\varepsilon\end{pmatrix}$$

anwendet und die Coëfficienten der neuen quadratischen Form durch A', B', C' bezeichnet. Also geht in der That die Form F durch die Substitution

$$\begin{pmatrix}\alpha\varepsilon, & \beta\varepsilon \\ \gamma\varepsilon. & \delta\varepsilon\end{pmatrix}$$

in die Form F' über. Ist nun speciell $\varepsilon = 1$, sind also f und f' eigentlich aequivalent, so sind auch F und F' aequivalent und gehen durch die Substitution

$$\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$$

in einander über. Ist hingegen $\varepsilon = -1$, so hat man die Transformation $\begin{pmatrix}-\alpha, & -\beta \\ -\gamma, & -\delta\end{pmatrix}$ beim Übergange von F zu F'; und diese kann durch die andere $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ ersetzt werden: folglich sind F und F' mit f und f' zugleich uneigentlich aequivalent.

Bezeichnet man die Determinanten von f und f', nämlich die Verbindungen

$$a^2d^2 - 3b^2c^2 + 4ac^3 + 4db^3 - 6abcd \quad \text{und}$$
$$a'^2d'^2 - 3b'^2c'^2 + 4a'c'^3 + 4d'b'^3 - 6a'b'c'd'$$

durch D und D', so hat man, wie sich aus dem obigen Beweise mit ergiebt, die höchst einfache Relation

$$11.\quad D' = (\alpha\delta - \beta\gamma)^6.D,$$

mithin für den Fall der Aequivalenz:

$$D' = D.$$

„*Also haben aequivalente cubische Formen aequivalente determinirende Formen und dieselbe Determinante.*"

Der eben bewiesene Satz kann als ein Fundamentalsatz für die Theorie der cubischen Formen angesehen werden, denn er begründet eine höchst einfache Eintheilung und Classificirung sämmtlicher cubischen Formen. In der

That: da alle Formen derselben Classe dieselbe Determinante haben, so zerfallen alle möglichen cubischen Formen, die zu einer gegebenen Determinante D gehören, in eine bestimmte Anzahl K von Classen, die auch Null sein könnte, wenn es etwa gar keine cubischen Formen mit der Determinante D geben sollte. Betrachtet man nun wiederum die sämmtlichen zur Determinante $D = B^2 - 4AC$ gehörigen quadratischen Formen

$$Ax^2 + Bxy + Cy^2,$$

so constituiren diese ebenfalls eine Anzahl h von Classen

$$\Gamma_1, \quad \Gamma_2, \quad \Gamma_3, \quad \ldots . \quad \Gamma_h,$$

welche nach *Dirichlet's* genialen Untersuchungen für eine negative Determinante von der Anzahl der Quadratreste für den Modul D abhängt, die unter einer gewissen Grenze liegen, und für eine positive Determinante von dem Exponenten der aus der Kreistheilung sich ergebenden Auflösung der *Pell*schen Gleichung. Da aber die determinirenden Formen aller aequivalenten cubischen Formen in dieselbe Classe gehören, während umgekehrt nicht alle cubischen Formen mit aequivalenten determinirenden Formen aequivalent sein müssen, so wird man für jede der obigen Classen quadratischer Formen Γ_n eine zugehörige Anzahl k_n (die auch Null sein kann) von Classen zugehöriger cubischer Formen haben, deren determinirende Formen alle zu der Classe Γ_n gehören, und es ist dann

$$k_1 + k_2 + \ldots . + k_n = K.$$

Man erhält also auf diesem Wege eine merkwürdige Doppel-Eintheilung sämmtlicher Classen cubischer Formen, indem man zuerst jedesmal alle diejenigen zusammenfafst, deren determinirende Formen aequivalent sind, und dann auf's Neue jedesmal alle zu derselben Determinante gehörenden zu einer höhern Ordnung vereinigt.

§. 4.

In der Theorie der quadratischen Formen wird gezeigt, dafs, wenn zwei Formen aequivalent sind, es gewöhnlich einige, zuweilen unendlich viele Transformationen giebt, durch welche die beiden Formen in einander übergehen können. Dieser Umstand kann bei den cubischen Formen nie eintreten, sondern wenn zwei cubische Formen aequivalent sind, so kann man nur durch *eine einzige Transformation* von der einen zur andern gelangen.

Es seien

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3 = (a, b, c, d) \text{ und}$$
$$f' = a'x'^3 + 3b'x'^2y' + 3c'x'y'^2 + d'y'^3 = (a', b', c', d')$$

zwei aequivalente cubische Formen, und

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

eine Transformation von f in f'. Um nun den Satz in aller Strenge zu erweisen, dafs nämlich keine zweite von der Transformation $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ verschiedene Transformation von f in f' existirt, mufs man mehrere Fälle unterscheiden.

Es sei zuerst die Determinante D der beiden cubischen Formen eine positive Zahl. Da in diesem Falle die cubische Gleichung

$$L = ax^3 + 3bx^2 + 3cx + d = 0,$$

so wie die andere

$$L' = a'x^3 + 3b'x^2 + 3c'x + d' = 0,$$

eine reelle und zwei imaginäre Wurzeln hat, so sei die reelle Wurzel $\frac{p}{p'}$ und die beiden imaginären $\frac{q+ri,\ q-ri}{b'+ri,\ q'-r'i}$.

Nachdem man diese Wurzeln gefunden, kann man die Formen f und $f,$ in lineare Factoren zerlegen, und setzen:

$$\left.\begin{array}{l} f = a[x-py][x-(q+ri)y][x-(q-ri)y] \\ f' = a'[x'-p'y'][x'-(q'+r'i)y'][x'-(q'-r'i)y'] \end{array}\right\} i = \sqrt{-1}.$$

Wendet man nun in der That auf f die Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ an, so kommt

$$a[(\alpha-\gamma p)x' + (\beta-\delta p)y'][(\alpha-\gamma q-\gamma ri)x' + (\beta-\delta q-\delta ri)y']$$
$$\times[(\alpha-\gamma q+\gamma ri)x' + (\beta-\delta q-\delta ri)y'].$$

Dieser Ausdruck mufs also $= f'$ sein. Umgekehrt: setzt man den gefundenen Ausdruck

$$= f' = a'[x'-p'y'][x'-(q'+r'i)y'][x'-(q'-r'i)y'],$$

so hat man eine Gleichung, welche in Verbindung mit der Gleichung

$$\alpha\delta - \beta\gamma = 1,$$

nach α, β, γ, δ als Unbekannten aufgelöset, alle Transformationen von f in f', wenn es deren mehrere geben sollte, liefern mufs.

Es läfst sich nun zeigen, dafs sich aus diesen Gleichungen höchstens zwei Systeme für α, β, γ, δ bestimmen lassen.

In der That: da man nur den reellen Factor mit dem reellen und die imaginären unter einander vergleichen kann, so darf man nur setzen:

1. $$a' = a(\alpha-\gamma p)(\alpha-\gamma q-\gamma ri)(\alpha-\gamma q+\gamma ri),$$
2. $$\frac{\beta-\delta p}{\alpha-\gamma p} = -\frac{a'}{a}p',$$



3. $\frac{\beta-\delta q-\delta ri}{\alpha-\gamma q-\gamma ri} = -\frac{a'}{a}(q' \pm r'i)$, d. h. entweder $= -\frac{a'}{a}(q'+r'i)$

oder $= -\frac{a'}{a}(q'-r'i)$,

4. und $\alpha\delta-\beta\gamma = 1$.

Die Gleichung (3.), mit irgend einem der beiden Vorzeichen von r' genommen, repräsentirt jedesmal zwei Gleichungen, da man den reellen Theil mit dem reellen, den imaginären mit dem imaginären vergleichen mufs. Auf diese Weise erhält man aus den beiden Gleichungen (2.) und (3.) drei lineare Gleichungen zur Bestimmung der Werthe von

$$\frac{\alpha}{\beta},\ \frac{\gamma}{\beta},\ \frac{\delta}{\beta};$$

also jedesmal, sowohl für $+r'$ als $-r'$, ein einziges System dieser Werthe. Es sei eins dieser beiden Systeme

$$\lambda,\ \nu,\ \varrho,$$

so erhält man aus der Gleichung $\alpha\delta-\beta\gamma=1$:

$$\frac{\alpha}{\beta}\cdot\frac{\delta}{\beta}-\frac{\gamma}{\beta} = \frac{1}{\beta^2},\quad \text{also}\quad \beta^2 = \frac{1}{\lambda\varrho-\nu}.$$

Von den beiden Werthen β und $-\beta$, die dieser Gleichung genügen, darf man nur den einen nehmen; denn da man aus jedem dieser beiden Werthe die Werthe von α, γ, δ vollständig bestimmt, nämlich aus dem Werthe β, $\alpha=\lambda\beta$, $\gamma=\nu\beta$, $\delta=\varrho\beta$, und aus dem negativen $-\beta$, $\alpha=-\lambda\beta$, $\gamma=-\nu\beta$, $\delta=-\varrho\beta$, so müfste es, sollten beide Werthe der Quadratwurzel zulässig sein, möglich sein, zugleich durch zwei Substitutionen von der Form

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\quad \begin{pmatrix}-\alpha, & -\beta\\ -\gamma, & -\delta\end{pmatrix}$$

von einer cubischen Form zu einer ihr aequivalenten überzugehen. Da die Unmöglichkeit dieses Letzteren sich aus dem blofsen Anblick der Gleichungen (7.) ergiebt (§. 1.), so folgt, dafs zu jedem der beiden entgegengesetzten Werthe von r höchstens *ein* System α, β, γ, δ gehört, also dafs im Ganzen höchstens zwei solcher Systeme existiren können.

Ich habe im Vorhergehenden bewiesen, dafs eine cubische Form mit positiver Determinante nie mehr als zwei Transformationen in eine ihr aequivalente zuläfst. Um nun zu zeigen, dafs nie zwei, sondern immer nur eine Transformation existirt, beweise ich, dafs aus der Annahme zweier Transformationen zwischen zwei aequivalenten Formen sich zwei Formen finden lassen, die durch *drei* verschiedene Transformationen in einander übergehen;

was dem Bewiesenen widerstreitet. Angenommen also, es gingen die Formen f und f' durch die beiden verschiedenen Transformationen

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = t_1, \quad \begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix} = t_2$$

in einander über. Man bilde die reciproke Transformation von t_1, nämlich

$$t_3 = \begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix},$$

durch welche f' in f übergeht, und verbinde sie mit t_2, so erhält man die neue Transformation

$$\tau_1 = \begin{pmatrix}\alpha'\delta-\beta'\gamma, & -\alpha'\beta+\beta'\alpha\\ \gamma'\delta-\delta'\beta, & -\gamma'\beta+\delta'\alpha\end{pmatrix},$$

durch welche f in f, d. h. f in sich selbst übergeht. Auf der andern Seite bilde man die reciproke Transformation von t_2 und verbinde sie mit t_1, so erhält man wiederum eine Transformation

$$\tau_2 = \begin{pmatrix}\alpha\delta'-\beta\gamma', & -\alpha\beta'+\beta\alpha'\\ \gamma\delta'-\delta\gamma', & -\gamma\beta'+\delta\alpha'\end{pmatrix},$$

durch welche f in sich selbst übergeht. Da sich zu diesen beiden Transformationen τ_1 und τ_2 noch die evidente

$$\tau_3 = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$$

gesellt, so würde man also *drei verschiedene* *) Transformationen haben, durch welche f in sich selbst übergehen könnte; was dem Bewiesenen widerstreitet.

Zweitens sei D negativ. Bezeichnen wir die determinirenden quadratischen Formen der beiden cubischen Formen f und f' durch F und F', so mufs jede Transformation, durch welche f in f' übergeht, auch F in F' übergehen lassen. Untersuchen wir nun, auf wie viele Arten die beiden quadratischen Formen F und F', oder, was dasselbe ist, die beiden quadratischen Formen

$$(2A,\ B,\ 2C) \quad \text{und} \quad (2A',\ B',\ 2C')$$

(nach der Bezeichnung von *Gaufs*) in einander übergehen können, so finden wir, dafs, mit Ausnahme weniger specieller Fälle, in welchen 4 oder 6 Transformationen stattfinden, und die wir der Kürze halber gegenwärtig bei Seite lassen wollen, die beiden quadratischen Formen nur durch zwei. und zwar durch zwei entgegengesetzte Transformationen (*Gaufs Disq. Art. 179.*)

$$\tau = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \quad \tau' = \begin{pmatrix}-\alpha, & -\beta\\ -\gamma, & -\delta\end{pmatrix}$$

*) Dafs sie alle drei verschieden sein müssen, läfst sich sehr leicht indirect nachweisen.



in einander übergehen. Bemerken wir nun, dafs zwei aequivalente cubische Formen nie durch zwei entgegengesetzte Transformationen zugleich in einander übergehen können, weil die Form f durch die Transformation τ' in $-f'$ übergeht, sobald sie durch die Transformation τ in f' verwandelt wird, so findet sich unser Satz auch für diesen Fall erwiesen.

§. 5.

Lehrsatz. Der vierfache Cubus des ersten Coëfficienten der determinirenden quadratischen Form einer zur Determinante D gehörigen cubischen Form ist immer durch die quadratische Grundform

$$U^2 - DV^2$$

darstellbar."

Die cubische Form sei $f = ax^3 + 3bx^2y + 3cxy^2 + dy^3$; alsdann ist der erste Coëfficient ihrer determinirenden quadratischen Form $b^2 - ac = A$, und die Determinante

$$D = a^2d^2 - 3b^2c^2 + 4ac^3 + 4db^3 - 6abcd;$$

also hat man die identische Gleichung

$$1. \quad (3abc - 2b^3 - a^2d)^2 - Da^2 = 4A^3,$$

von deren Richtigkeit man sich durch die Entwickelung überzeugt. In dieser Formel liegt aber der Beweis des Lehrsatzes.

Es sei nun A' eine beliebige, durch die Form

$$Ax^2 + Bxy + Cy^2 = F$$

darstellbare Zahl; dann kann man F in eine zweite quadratische Form transformiren, deren erster Coëfficient $= A'$ ist. Dieselbe sei daher

$$A'x'^2 + B'x'y' + C'y'^2 = F'.$$

Wendet man nun die nämliche Transformation, durch welche man F' aus F erhielt, auf die cubische Form f an, so erhält man eine zweite cubische Form f', und es wird nach dem in §. 3. Bewiesenen F' die determinirende quadratische Form von der cubischen Form f' sein. Da nun A' der erste Coëfficient von F', und D die Determinante von f' ist, so folgt aus dem obigen Lehrsatze, dafs $4A'^3$ durch die quadratische Grundform $U^2 - DV^2$ darstellbar sein wird. Man hat demnach folgenden allgemeinen Satz.

Lehrsatz. „Wenn eine Zahl N durch die determinirende Form einer cubischen Form mit der Determinante D darstellbar ist, so ist ihr vierfacher Cubus $4N^3$ durch die quadratische Grundform

$$U^2 - DV^2$$

darstellbar."

Auf ganz ähnliche Weise läfst sich auch der folgende Satz beweisen:

Lehrsatz. „Wenn eine Zahl durch die determinirende Form $Ax^2 + Bxy + Cy^2 = F$ einer cubischen Form $f = (a, b, c, d)$ mit der Determinante D darstellbar ist, so ist ihr *Quadrat* durch die entgegengesetzte Form $Ax^2 - Bxy + Cy^2$ darstellbar."

Denn wenn A' irgend eine durch die Form F darstellbare Zahl bezeichnet, so läfst sich die Form F in eine aequivalente Form F' transformiren, deren erster Coëfficient der Zahl A' gleich ist; es sei $F' = A'x'^2 + B'x'y' + C'y'^2$. Durch die nämliche Transformation erhält man aber nach §. 3. aus f die neue cubische Form

$$f' = a'x'^3 + 3b'x'^2y' + 3c'x'y'^2 + d'y'^3,$$

deren determinirende Form die Form F' ist. Man hat nun nach §. 1. die nachstehenden Gleichungen:

$$A' = b'^2 - a'c', \quad B' = b'c' - a'd', \quad C' = c'^2 - b'd',$$

und aus diesen ergeben sich unmittelbar auf rein algebraischem Wege die folgenden drei:

$$2. \quad A'^2 = A'b'^2 - B'a'b' + C'a'^2,$$
$$3. \quad A'C' = A'c'^2 - B'b'c' + C'c'^2,$$
$$4. \quad C'^2 = A'd'^2 - B'd'c' + C'c'^2.$$

Aus der Gleichung (2.) ersieht man aber, dafs A'^2 durch die Form

$$A'x^2 - B'xy + C'y^2$$

repräsentirt werden kann. Da nun diese Form der Form

$$Ax^2 - Bxy + Cy^2$$

aequivalent ist, so mufs A'^2 ebenfalls durch diese letztere Form darstellbar sein; was zu beweisen war.

§. 6.

Mit Hülfe der vorhergehenden Sätze wird es uns möglich sein, einen merkwürdigen Zusammenhang nachzuweisen, der zwischen der Theorie der *cubischen Formen* und der Theorie der *Zusammensetzung* oder *Multiplication* der quadratischen Formen stattfindet. Da jedoch diese Untersuchung in ihrer ganzen Allgemeinheit, d. h. für jede beliebige Determinante, ein näheres Eingehen in die Natur dieser letzteren Theorie erfordert, welche, so viel ich weifs, seit ihrer Entdeckung durch den berühmten Verfasser der „Disquisitiones" noch durch Niemand weiter ausgebildet worden ist, so sei es uns erlaubt, den Gegenstand für's Erste in einem speciellen Falle zu behandeln.

Wir nehmen den Fall, in welchem die Determinante von der Form $D = -4p$ und p eine positive Primzahl von der Form $4n+3$ ist, welche, als Determinante einer quadratischen Form angesehen, zu denen gehört, die *Gaufs* regelmäfsige nennt.

Ich stelle mir jetzt die Aufgabe: alle quadratischen Formen zu finden, welche determinirende Formen zu cubischen Formen mit der Determinante $-4p$ sein können; und da jede quadratische Form, die diese Eigenschaft besitzt, sie mit allen ihr aequivalenten theilt (§. 3.), so wird es genügen, alle nicht aequivalenten quadratischen Formen dieser Gattung aufzusuchen. Es sei

$$1.\quad ax^3+3bx^2y+3cxy^2+dy^3 = f$$

eine cubische Form, deren determinirende quadratische Form

$$2.\quad Ax^2+Bxy+Cy^2 = F$$

und deren Determinante $= B^2-4AC = -4p$ ist. Alsdann mufs zuerst B eine gerade Zahl sein, weil sonst die Gleichung $B^2-4AC = -4p$ nicht existiren kann. Es ist also $B = 2\mathrm{B}$, so dafs

$$3.\quad \mathrm{B}^2-AC = -p$$

ist. Hierauf ist $-p$ die Determinante der quadratischen Formen

$$4.\quad (A, \mathrm{B}, C) = F;$$

nach der Bezeichnung von *Gaufs*.

Nach dem Lehrsatze des vorigen Paragraphen ist nun der vierfache Cubus jeder durch F darstellbaren Zahl durch die Form x^2+4py^2 darstellbar: also wird der einfache Cubus jeder durch F darstellbaren Zahl durch die Form x^2+py^2, mithin allgemein durch alle Formen der zur Determinante $-p$ gehörigen Hauptclasse darstellbar sein; oder, noch allgemeiner: es werden die Cuben aller Zahlen, welche sich durch diejenige Classe darstellen lassen, welche die Form F enthält, durch die Hauptclasse darstellbar sein.

Unter der für die Primzahl p gemachten Annahme werden sich alle zur Determinante $-p$ gehörigen Classen quadratischer Formen durch successives Zusammensetzen aus einer derselben bilden lassen. Nennen wir $h = 2\lambda+1$ die Anzahl dieser Classen, welche wir durch K bezeichnen und durch Indices von einander unterscheiden wollen, so lassen sich dieselben immer in folgende Ordnung bringen:

$$5.\quad K_{-\lambda},\ K_{-(\lambda-1)},\ \ldots\ K_{-1},\ K_0,\ K_1,\ \ldots\ K_{\lambda-1},\ K_\lambda;$$

welche Reihe als in sich zurückkehrend zu betrachten ist, so dafs auf K_λ wieder $K_{-\lambda}$ folgt, und wo jede Classe aus der vorhergehenden und der Classe K_1 zusammengesetzt ist, K_0 die Hauptclasse vorstellt und entgegengesetzten

Classen entgegengesetzte Indices entsprechen. Nun hat Hr. Professor *Lejeune Dirichlet*, der Verfasser des Beweises über die arithmetische Progression, durch eine neue Anwendung seines herrlichen Princips gezeigt, dafs jede dieser Classen unendlich viele Primzahlen repräsentirt: wir können uns dieselben daher sämmtlich durch solche Formen repräsentirt vorstellen, deren erste Coëfficienten Primzahlen sind.

Es sei $(A, B, C) \backsim F_\mu$ und q, der erste Coëfficient von F_μ, eine ungerade Primzahl. Da nun q^3 durch die Classe K_0 darstellbar sein soll, so mufs der Index μ der Bedingung

$$6.\quad 3\mu \equiv 0 \pmod{k}$$

genügen. Andere Formen also, als diejenigen, welche diese Bedingung erfüllen, können für den in Rede stehenden Fall nicht determinirende Formen zu cubischen Formen bilden.

Auf der andern Seite werde ich zeigen, dafs allen quadratischen Classen, welche die Bedingung (6.) erfüllen, in der That cubische Classen entsprechen; und zwar jeder derselben nur eine einzige.

Es sei also F_μ eine quadratische Form, deren Index der Congruenz (6.) genügt, oder, was dasselbe ist, welche durch ihre Triplication die Hauptclasse hervorbringt, so dafs man

$$7.\quad q^3 = U^2 + p.V^2$$

setzen kann; wo U und V relative Primzahlen sind.

Dieses vorausgesetzt, betrachten wir die cubische Form

$$8.\quad Vx^3 + 3bx^2y + 3\,\frac{b^2-q}{V}\,xy^2 + \frac{b^3-3qb+2U}{V^2}\,y^3,$$

in welcher b eine noch vorläufig unbestimmt gelassene ganze Zahl vorstellt. Diese cubische Form genügt den Bedingungen, dafs der erste Coëfficient ihrer determinirenden quadratischen Form $= b^2 - V.\frac{b^2-q}{V} = q$ und dafs ihre Determinante $= 4\frac{U^2-q^3}{V^2} = -4p$ ist. Suchen wir jetzt b so zu bestimmen, dafs ihre beiden letzten Coëfficienten ganze Zahlen werden. Zu dem Ende mufs den beiden Congruenzen

$$9.\quad b^2 - q \equiv 0 \pmod{V},$$

$$10.\quad b^3 - 3qb + 2U \equiv 0 \pmod{V^2}$$

genügt werden.

Wenn wir den Ausdruck $b^3-3qb+2U$ durch $\varphi(b)$ bezeichnen, so ist der Differenzialquotient $\frac{d\varphi(b)}{db} = 3(b^2-q)$; was für die Auflösung der beiden



Congruenzen von Wichtigkeit ist. Ferner bemerke ich, dafs wegen der Gleichung (7.) q^3, also auch q zu V^2, mithin auch zu jedem in V enthaltenen Theiler quadratischer Rest sein wird. Beschäftigen wir uns nun mit der Auflösung der beiden Congruenzen.

I. Es sei l die höchste in V aufgehende Potenz einer ungeraden Primzahl. Dann genügen, wie bekannt, der Congruenz $b^2 \equiv q \pmod{l}$ zwei nach dem Modul l incongruente, dem Zeichen nach entgegengesetzte Werthe von b, die wir durch $\pm z$ bezeichnen. Bilden wir nun die Reihe der Zahlen

$$11. \quad z, \quad z+l, \quad z+2l, \quad \ldots. \quad z+(l-1)l,$$

so befindet sich unter denselben eine einzige, welche zugleich der Congruenz $b^2 \equiv q \pmod{l^2}$ genügt. Wird dieselbe mit ζ bezeichnet, so ist auch $\zeta^3 \equiv q\zeta \pmod{l^2}$, also $\varphi(\zeta) \equiv 2(U-q\zeta) \pmod{l^2}$. Nun folgt aus (7.) $q^3 \equiv U^2 \pmod{l^2}$, also ist $U^2 - q^2\zeta^2 \equiv 0 \pmod{l^2}$, d. h. $(U-q\zeta)(U+q\zeta)$ durch l^2 theilbar. Da nun diese beiden Factoren keinen in l enthaltenen gemeinschaftlichen Theiler haben können, weil derselbe sonst in ihrer Differenz $2U$, also in U und V zugleich aufgehen würde, so wird nothwendig einer der beiden Ausdrücke $U \mp q\zeta$ durch l^2 theilbar sein, während der andere zu l relative Primzahl ist. Das Zeichen von ζ kann demnach auf eine und nur auf eine Art so bestimmt werden, dafs $\varphi(\zeta) \equiv 0 \pmod{l^2}$. Der Werth $b = \zeta$ genügt dann den beiden Congruenzen

$$12. \quad b^2 - q \equiv 0 \pmod{l} \quad \text{und} \quad 13. \quad b^3 - 3qb + 2U \equiv 0 \pmod{l^2}.$$

Ich behaupte aber, dafs auch jeder Werth von der Form $\zeta + kl$, also jeder in der Reihe (11.) enthaltene Werth, wenn man das Zeichen von z schicklich wählt, diesen beiden Congruenzen genügen wird. In der That setze man $\zeta + kl$ in den Ausdruck $\varphi(b)$ statt b, so erhält man

$$\varphi(\zeta + kl) \equiv \varphi(\zeta) + kl \frac{d\varphi(\zeta)}{d\zeta} \pmod{l^2},$$

welches durch l^2 theilbar sein wird, weil $\varphi(\zeta)$ durch l^2 und $\frac{d\varphi(\zeta)}{d\zeta} = 3(\zeta^2 - q)$ durch l theilbar ist.

Als Resultat dieser Untersuchung ergiebt sich also, dafs für jede höchste in V enthaltene Potenz l einer ungeraden Primzahl immer eine und nur eine einzige ganze Zahl z existirt, die so beschaffen ist, dafs sie, mit allen ihr nach dem Modul l congruenten statt b gesetzt, die sämmtlichen Auflösungen der beiden Congruenzen (12. und 13.) giebt.

II. Es sei für den Fall, dafs V eine gerade Zahl ist, $2^\vartheta = l$ die höchste in V enthaltene Potenz von 2. Alsdann läfst sich durch ganz ähnliche Betrachtungen zeigen, dafs auch für diesen Werth von l den Congruenzen (12. u. 13.) ein einziger Werth von b mit allen ihm nach dem Modul l congruenten genügt. Wenn $\vartheta = 1$ oder $= 2$, also $l = 2$ oder $= 4$ ist, so sieht man sogleich, dafs dieser Werth $b = 1$ ist. Es sei $\vartheta \geqq 3$: alsdann existiren vier nach dem Modul l incongruente Werthe von b, die der Congruenz $b^2 \equiv q$ (mod. l) genügen; und wenn man einen derselben z nennt, so lassen sie sich auf folgende Art gruppiren:

14. $\quad +z, \quad -z, \quad z+2^{\vartheta-1}, \quad -z+2^{\vartheta-1}$ (*Gaufs* Disq. 103).

Von diesen 4 Werthen genügen aber nur zwei $\pm z$ zugleich der Congruenz $b^2 \equiv q$ (mod. l^2). Es sei also $z^2 \equiv q$ (mod. l^2); alsdann folgt wie oben

$$\varphi(z) \equiv 2(U - qz) \text{ (mod. } l^2\text{)},$$

und da wegen (7.) $q^3 \equiv U^2$ (mod. l^2), also $U^2 - q^2 z^2 \equiv 0$ (mod. l^2) ist, und die beiden Factoren $U \mp qz$ höchstens den gemeinschaftlichen Theiler 2 haben können, so wird sich das Zeichen von z immer auf eine und nur auf eine Art so bestimmen lassen, dafs $U - qz$ durch $\frac{1}{2} l^2$, also $\varphi(z)$ durch l^2 theilbar ist. Es bleibt noch zu zeigen, dafs der Werth $b = z + 2^{\vartheta-1}$ der Congruenz (13.) nicht genügen kann. Diese Annahme würde auf die Congruenz

$$\varphi(z) + 2^{\vartheta-1}.3(z^2 - q) + 2^{2\vartheta-2}.z \equiv 0 \text{ (mod. } 2^{2\vartheta}\text{)}$$

führen, welche nicht stattfinden kann, da q, also z, eine ungerade Zahl ist.

III. Stellt man sich nun V auf die Form

15. $\quad V = l.l'.l''....$

gebracht vor, wo l, l', l'' etc. Potenzen verschiedener Primzahlen sind, mit Einschlufs der 2, so lassen sich die Congruenzen (12. und 13.) nach jedem der Moduln l, l', l'', ... auflösen, und geben jedesmal eine einzige Lösung. Bezeichnen wir diese Lösungen nach den verschiedenen Moduln der Reihe nach, resp. durch z, z', z'' etc., und suchen dann eine Zahl, welche zugleich $\equiv z$ (mod. l), $\equiv z'$ (mod. l'), $\equiv z''$ (mod. l'') etc. ist, so wird dieselbe, statt b gesetzt, nothwendig den beiden Congruenzen (9. u. 10.) zugleich genügen; und alle anderen Zahlen, welche die nämliche Eigenschaft haben, werden ihr nach dem Modul V congruent sein.

Da nun ferner alle nach dem Modul V congruenten Werthe von b, in die cubische Form (8.) gesetzt, lauter aequivalente Formen hervorbringen, die durch Substitutionen von der folgenden Art:

16. $\quad x = x' + ky', \quad y = 0.x' + y',$

für welche

$$1.1 - k.0 = 1$$

ist, in einander übergehen, so werden wir auf diesem Wege immer zu einer, aber auch nur zu einer einzigen Classe cubischer Formen gelangen, welche allen Bedingungen genügt.

Zweitens läfst sich nachweisen, dafs es unmöglich ist, auf anderem Wege eine zweite Classe cubischer Formen zu entdecken, die dieselben Eigenschaften besitzt. Denn man stelle sich irgend eine cubische Form

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 = f$$

vor, deren determinirende quadratische Form zum ersten Coëfficienten q hat und deren Determinante $= -4p$ ist. Alsdann läfst sich f durch Zerlegung in lineare Factoren auf die Form

$$17. \quad f = \frac{1}{a^2}\left\{ax + [b - \sqrt[3]{(E + a\sqrt{-p})} - \sqrt[3]{(E - a\sqrt{-p})}]y\right\}$$
$$\times \left\{ax + [b - \varrho\sqrt[3]{(E + a\sqrt{-p})} - \varrho^2\sqrt[3]{(E - a\sqrt{-p})}]y\right\}$$
$$\times \left\{ax + [b - \varrho^2\sqrt[3]{(E + a\sqrt{-p})} - \varrho\sqrt[3]{(E - a\sqrt{-p})}]y\right\}$$

bringen, wo E eine ganze Zahl ist, die mit a keinen gemeinschaftlichen Theiler hat, $\varrho = \frac{1}{2}(-1 + \sqrt{-3})$ und

$$18. \quad E^2 + pa^2 = q^3$$

ist. Da nun die unbestimmte Gleichung $U^2 + pV^2 = q^3$ nur auf eine einzige Art in relativen Primzahlen lösbar ist, so mufs $E = U$ und $a = V$ sein. Bemerkt man dies und multiplicirt die drei Factoren in (17.) wirklich in einander, so wird man wieder zu der cubischen Form (8.) geführt, von welcher wir oben ausgegangen waren.

Aus allem diesen ergiebt sich nun Folgendes.

„Wenn p eine Primzahl von der Form $4n + 3$ ist und $-p$ zu den regelmäfsigen Determinanten gehört, so entspricht jeder Classe quadratischer Formen mit der Determinante $-p$, welche durch ihre Triplication die Hauptclasse hervorbringt, eine Classe cubischer Formen mit der Determinante $-4p$, während den übrigen quadratischen Classen keine cubischen Classen mit derselben Determinante entsprechen."

Mit diesem eleganten Satze schliefse ich diese erste Abtheilung, in welcher ich nur die Elemente eines ganz neuen Feldes der Zahlenlehre aufstellen wollte. Sollte ich mir schmeicheln dürfen, dafs dieser erste Versuch

eines Anfängers sich des Beifalls der Mathematiker erfreuen könnte, so würde ich mit Vergnügen die begonnene Arbeit fortsetzen; zumal da ich gerade die interessantesten Resultate zurückhalten mufste, auf welche die vollständige Theorie der Vertheilung der cubischen Classen auf die quadratischen führt, und die auf eine merkwürdige Weise von der Betrachtung derjenigen Formen abhängen, welche ganz allgemein, nicht blofs die Haupt- oder Grundform, sondern eine beliebige gegebene primitive quadratische Form durch ihre Triplication erzeugen.

Berlin im December 1843.

(Die Fortsetzung folgt.)

9.

Über eine merkwürdige identische Gleichung.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

Die Function von 4 Variabeln

$$1.\quad a^2d^2-3b^2c^2+4ac^3+4db^3-6abcd$$

besitzt neben andern merkwürdigen Eigenschaften auch diejenige, dafs ihr *Cubus* sich durch die *nämliche Function* ausdrücken läfst, wenn man den Variabeln Werthe giebt, die aus den obigen auf eine sehr einfache Weise zusammengesetzt sind. In der That findet die identische Gleichung

$$2.\quad (a^2d^2-3b^2c^2+4ac^3+4db^3-6abcd)^3 = A^2D^2-3B^2C^2+4AC^3+4DB^3-6ABCD$$

Statt, wenn gesetzt wird:

$$3.\quad \begin{cases} A = 3abc-a^2d-2b^3, \\ B = 2ac^2-abd-b^2c, \\ C = acd-2b^2d+bc^2, \\ D = ad^2-3bcd+2c^3. \end{cases}$$

Diese Formel kann als eine Art Seitenstück angesehen werden zu der merkwürdigen Gleichung, die *Lagrange* in den Berliner Memoiren aufgestellt hat, und welche sich folgendermafsen schreiben läfst:

$$4.\quad [pp'p''+2qq'q''-pq^2-p'q'^2-p''q''^2]^2 = PP'P''+2QQ'Q''-PQ^2-P'Q'^2-P''Q''^2,$$

wo gesetzt ist:

$$5.\quad \begin{cases} P = p'p''-q^2, & P' = pp''-q'^2, & P'' = pp'-q''^2; \\ Q = q'q''-pq, & Q' = qq''-p'q', & Q'' = qq'-p''q''. \end{cases}$$

Es scheint, man müsse dieser Gattung von identischen Gleichungen eine um so gröfsere Wichtigkeit zuschreiben, als man keine allgemeine Methode zu ihrer Auffindung besitzt, und weil dieselben namentlich in der Zahlenlehre oft die Grundlage zu ganzen Theorieen bilden; in welcher Hinsicht sich auf die Theorieen der quadratischen und ternären Formen, so wie auf diejenige der Zerlegung einer Zahl in die Summe von vier Quadraten und andere verweisen läfst.

Nachschrift. Wenn man aus den vier Ausdrücken A, B, C, D vier neue A', B', C', D' auf die nämliche Weise zusammensetzt, wie A, B, C, D aus a, b, c, d entstanden sind, d. h. wenn man setzt:

$$\begin{aligned} A' &= 3ABC - A^2 D - 2B^3, \\ B' &= 2AC^2 - ABD - B^2 C, \\ C' &= ACD - 2B^2 D + BC^2, \\ D' &= AD^2 - 3BCD + 2C^3, \end{aligned}$$

so lassen sich diese neuen Verbindungen A', B', C', D' auf eine sehr einfache und merkwürdige Weise in die ursprünglichen Elemente a, b, c, d ausdrücken. Man findet nämlich, wenn man die Werthe von A, B, C, D einführt, nach allen Reductionen:

$$A' = a\Delta^2, \quad B' = b\Delta^2, \quad C' = c\Delta^2, \quad D' = d\Delta^2,$$

wo der Kürze halber

$$\Delta = a^2 d^2 - 3b^2 c^2 + 4ac^3 + 4db^3 - 6abcd$$

gesetzt ist.

10.

Encyklopädische und elementare Darstellung der Theorie der Zahlen.

(Vom Herausgeber dieses Journals.)

(Fortsetzung der Abhandlung No. 2. im vorigen Heft.)

---

§. 21.

Erläuterung.

Jede theilbare ganze Zahl z kann z. B. durch

$$z = a^\alpha b^\beta c^\gamma d^\delta \ldots\ldots n^\nu$$

ausgedrückt werden, wo die Factoren $a, b, c, d \ldots\ldots n$ von z entweder theilbare, unter einander theilerverwandte, oder theilerfremde, oder auch untheilbare ganze Zahlen sein *können*, die Exponenten $\alpha, \beta, \gamma, \ldots\ldots \nu$ aber *nothwendig* ganze *positive* Zahlen sind.

Denn eine theilbare ganze Zahl z ist nichts anderes als das *Product* anderer ganzen Zahlen, die selbst wiederum theilbar, unter einander theilerverwandt, oder theilerfremd, oder auch untheilbar sein können. Diejenigen unter diesen Factoren, welche einander *gleich sind*, wie z. B. alle die, welche gleich a sind, geben für sich, in einander multiplicirt, eine *Potenz* mit ganzzahligen positiven Exponenten. Z. B. wenn a αmal als Factor vorkommt, so entsteht daraus die Potenz a^α; b, wenn es β*mal* vorkommt, giebt die Potenz b^β u. s. w., und das Product aller dieser Potenzen macht die Zahl z aus.

§. 22.

Lehrsatz.

I. *Wenn von einer ganzen Zahl* z, *die nach* (§. 21.) *immer durch*

$$1. \quad z = a^\alpha b^\beta c^\gamma d^\delta \ldots\ldots n^\nu$$

ausgedrückt werden kann, keiner der Factoren a, b, c, d, ... n *mit einer andern beliebigen ganzen Zahl* u *theilerverwandt ist, so ist auch* z *selbst mit* u *nicht theilerverwandt, sondern zu* u *theilerfremd.*

II. *Wenn von einer ganzen Zahl*

$$2. \quad z = a^\alpha b^\beta c^\gamma d^\delta \ldots n^\nu$$

keiner der Factoren a, b, c, d, ... n *mit irgend einem der Factoren* a_1, b_1, c_1, ... k_1 *einer andern ganzen Zahl*

$$3. \quad u = a_1^{\alpha_1} b_1^{\beta_1} c_1^{\gamma_1} \ldots\ldots k_1^{\varkappa_1}$$

theilerverwandt ist, so sind auch z *und* u *selbst nicht theilerverwandt, sondern zu einander theilerfremd.*

III. *Wenn die Factoren* a, b, c, ... n *und* a_1, b_1, c_1, ... k_1 *der beiden Zahlen* z *und* u (2. u. 3.) *sämmtlich Stammzahlen sind, und keiner der Factoren* a, b, c, ... n *ist irgend einem der Factoren* a_1, b_1, c_1, ... k_1 *gleich, so sind* z *und* u *zu einander theilerfremd.*

Beweis von I. *A.* Da nach der Voraussetzung a in (1.) zu u theilerfremd ist, so ist es nach (§. 20. I.) auch das *Product* $a.a$ oder a^2. Folglich sind a und a^2 *beide* zu u theilerfremd. Also ist es nach (§. 20. I.) auch ihr *Product* $a.a^2$ oder a^3. Also sind a und a^3 *beide* zu u theilerfremd, und folglich ist es auch ihr *Product* $a.a^3 = a^4$. Und so weiter. Also ist zuletzt a^α zu u theilerfremd.

B. Aus gleichen Gründen sind, da $b, c, d, \ldots n$ sämmtlich der Voraussetzung nach zu u theilerfremd sind, auch b^β, c^γ, d^δ, ... n^ν zu u theilerfremd. U. s. w.

C. Da weiter z. B. a^α und b^β *beide* zu u theilerfremd sind, so ist es nach (§. 20. I.) auch ihr *Product* $a^\alpha b^\beta$. Und da demzufolge $a^\alpha b^\beta$ und c^γ (*B.*) *beide* zu u theilerfremd sind, so ist es nach (§. 20. I.) auch ihr *Product* $a^\alpha b^\beta c^\gamma$. So ist weiter, aus gleichen Gründen, $a^\alpha b^\beta c^\gamma d^\delta$ u. s. w. und folglich zuletzt $z = a^\alpha b^\beta c^\gamma d^\delta \ldots n^\nu$ nothwendig zu u theilerfremd; wie es (I.) behauptet.

Beweis von II. *D.* Da nach der Voraussetzung in (II.) keiner der Factoren a_1, b_1, c_1, ... k_1 von u z. B. mit dem Factor a von z theilerverwandt ist, so ist nach (I.) auch u selbst mit a *nicht* theilerverwandt. Aus demselben Grunde ist u auch mit keinem andern der Factoren von z theilerverwandt. Also ist kein Factor von z mit u theilerverwandt und folglich nach (I.) auch z selbst nicht; gemäfs (II.).

Beweis von III. Nur *einander gleiche* Stammzahlen sind theilerverwandt; denn keine Stammzahl hat einen andern Theiler >1, als sich selbst. Nun soll in (III.) keiner der Stammfactoren von z irgend einem der Stammfactoren von u *gleich sein:* also ist keiner der Factoren von z irgend einem der Factoren von u theilerverwandt, und folglich sind nach (II.) z und u selbst einander *nicht* theilerverwandt, sondern theilerfremd.

Anm. Der Beweis von (I.) beruht auf der wiederholten Anwendung des Lehrsatzes (§. 20. I.). Der Beweis von (II.) beruht auf der Anwendung von (I.) zunächst auf die einzelnen Factoren von z; der Beweis von (III.)

beruht darauf, dafs hier die Factoren von u und z von selbst in dem in (II.) vorausgesetzten Falle sind.

§. 23.

Lehrsatz.

Der gröfste Gemeintheiler zweier ganzen Zahlen z *und* u *ist das Product aller derjenigen Stammfactoren, welche* z *und* u *gemein haben.*

Beispiel. Der gröfste Gemeintheiler von

1. $z = 3^8.7^4.11.13^3.17^2$ und $u = 3^7.7^2.17^3.19^2$

ist

2. $3^5.7^2.17^2$.

Nur die Stammfactoren von (2.) kommen in z und u *zugleich* vor.

Beweis. *A.* Man bezeichne das Product *aller* Stammfactoren, welche z und u *gemein haben*, durch v, die Producte der *übrigen* Stammfactoren in z und in u durch z_1 und u_1, so dafs also

3. $\frac{z}{u} = \frac{v.z_1}{v.u_1}$

ist. Hier ist $\frac{v.z_1}{v.u_1}$ nichts anderes als der Bruch $\frac{z_1}{u_1}$ im Zähler und Nenner durch die *gleiche* Zahl v multiplicirt. Also ist nach (§. 13. *I.* 8.)

4. $\frac{z}{u} = \frac{z_1}{u_1}$.

B. Nach der Voraussetzung sind in v *alle* diejenigen Stammfactoren von u enthalten, die zugleich in z vorkommen. Also sind alle Stammfactoren, die u_1 noch sonst enthält, von allen, die noch in z_1 vorkommen, *verschieden.* Deshalb sind denn zufolge (§. 22. III.) z_1 und u_1 in (4.) *theilerfremd;* das heifst, sie haben keinen Factor >1 weiter gemein. Folglich ist v, nemlich das Product *aller* Stammfactoren, welche z und u *gemein haben*, der *gröfste* Gemeintheiler von z und u; wie es der Lehrsatz behauptet.

§. 24.

Lehrsatz.

Wenn eine ganze Zahl z *mit einer andern ganzen Zahl* u *aufgeht, so müssen unter den Stammfactoren von* z *nothwendig alle Stammfactoren von* u *ohne Ausnahme vorkommen.*

Beweis. *A.* Es sei

1. $z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu$,

wo $a, b, c, \dots n$ *Stammzahlen* sind. Käme in u irgend ein Stammfactor

v vor, der keinem der Stammfactoren $a, b, c, \ldots. n$ *gleich* wäre, so ginge v in *keinen* dieser Factoren auf, also zuerst in a nicht. Deshalb geht denn v nach (§. 20. II.) auch in $a.a = a^2$ nicht auf; folglich auch nicht in $a.a^2 = a^3$ u. s. w., und folglich nicht in a^α. Auch in b geht v nicht auf, folglich aus gleichen Gründen auch in b^β nicht. Eben so nicht in c^γ, d^δ, ... n^ν, also auch gemäfs (§. 20. II.) in $a^\alpha b^\beta$ nicht, und auch nicht in $a^\alpha b^\beta . c^\gamma = a^\alpha b^\beta c^\gamma$ u. s. w., mithin auch in z selbst nicht.

B. Wenn nun aber z mit dem *Factor* v von u nicht aufgeht, so geht auch nach (§. 15. I.) u *selbst* in z nicht auf. Es ist also, wenn u in z aufgeht, nicht möglich, dafs u irgend einen Factor v habe, der von allen Stammfactoren von z verschieden wäre.

§. 25.

Lehrsatz.

I. *Wenn eine ganze Zahl* u *in das* ***Product*** $z_1 z_2$ *zweier ganzen Zahlen* z_1 *und* z_2 *aufgeht, und sie ist zu einer derselben, z. B. zu* z_1, ***theilerfremd,*** *so mufs sie nothwendig in die andere* z_2 ***aufgehen.***

II. *Ist dagegen* u *zu keiner der beiden Zahlen* z_1 *und* z_2 *theilerfremd, so kann* u *in das Product* $z_1 z_2$ *aufgehen, obgleich weder in* z_1 *noch in* z_2.

Beispiele. *No. 1.* zu I. $u = 16$ geht in $z_1 z_2 = 75.144 = 10800$ auf und ist zu $z_1 = 75$ *theilerfremd.* Deshalb mufs $u = 16$ in $z_2 = 144$ aufgehen.

No. 2. zu II. $u = 120$ ist weder zu $z_1 = 75$ noch zu $z_2 = 144$ theilerfremd und geht in $z_1 z_2 = 75.144 = 10800$ auf, obgleich weder in 75, noch in 144.

Beweis von I. *A.* Da u in das Product $z_1 z_2$ aufgehen soll, so müssen nach (§. 24.) in diesem Product *alle* Stammfactoren von u ohne Ausnahme vorkommen. Nun sollen z_1 und u *theilerfremd* sein, das heifst, es soll in z_1 *keiner* der Stammfactoren von u vorkommen. Also müssen *alle* Stammfactoren von u ohne Ausnahme in z_2 allein vorhanden sein, und folglich mufs u selbst, welches das Product seiner Stammfactoren ist, nothwendig in z_2 aufgehen.

Beweis von II. *B.* Sind u und z_1 *nicht theilerfremd*, so hat z_1 mit u Stammfactoren gemein; angenommen *nicht alle.* Enthält nun das Product $z_1 z_2$ die verschiedenen Stammfactoren von u zusammen nur gerade *so oft*, als sie in u vorkommen, welches schon hinreicht, damit u in $z_1 z_2$ auf-

gehe, so enthält z_2 nicht mehr *alle* Stammfactoren von u, indem z_1 schon einige davon wegnimmt. Also geht in diesem Falle nach (§. 24.) u nicht mehr in z_2 auf, eben so wenig wie in z_1, obschon gleichwohl in $z_1 z_2$.

§. 26.

Lehrsatz.

Wenn eine ganze Zahl z *mit jeder der verschiedenen Zahlen* v_1, v_2, v_3, ... v_n ***aufgeht****, so geht sie auch mit ihrem* ***Product***

$$1. \quad u = v_1 v_2 v_3 \ldots\ldots v_n$$

auf, jedoch nothwendig ***nur*** *dann, wenn keine der Zahlen* v *einen Stammfactor mit der andern gemein hat.*

Beispiel 1. Die Zahl $z = 75600$ geht mit jeder der drei Zahlen 8, 21 und 25 auf, deren keine einen Stammfactor mit der andern gemein hat. Deshalb geht sie *nothwendig* auch mit ihrem *Product* $8.21.25 = 4200$ auf.

2. Die Zahl $z = 75600$ geht mit jeder der drei Zahlen 12, 36 und 105 auf, welche Stammfactoren mit einander gemein haben, nicht aber mit ihrem Product $12.36.105 = 45360$.

Beweis. *A.* Da nach der Voraussetzung z mit v_1, v_2, v_3, ... v_n aufgehen soll, so müssen nach (§. 24.) unter den Stammfactoren von z *alle* Stammfactoren von v_1, v_2, v_3, ... v_n ohne Ausnahme, also *alle* Stammfactoren von u sein.

B. Es geht also nothwendig z eben sowohl z. B. mit v_1 auf, als u. Setzt man daher

$$2. \quad z = v_1 z_1,$$

so ist z_1 eine *ganze* Zahl.

C. Sind nun alle Stammfactoren jedes der Factoren v von denen der übrigen *verschieden*, so wird durch die Division von z durch v_1 *keiner* der Stammfactoren von v_2, v_3, ... v_n weggenommen; mithin enthält z_1 in (2.) noch alle diese letzteren Stammfactoren vollständig.

D. Nun ist zufolge (2.)

$$3. \quad \frac{z}{u} = \frac{v_1 z_1}{v_1 v_2 v_3 \ldots\ldots v_n} = \frac{z_1}{v_2 v_3 v_4 \ldots\ldots v_n} \quad (§. 13.\ I.\ 8.)$$

und es kann z_1, da es noch alle Stammfactoren von v_2, v_3, ... v_n enthält, durch v_2 dividirt werden, so dafs, wenn man

$$4. \quad z_1 = v_2 z_2$$

setzt, z_2 eine *ganze* Zahl ist. Und zwar enthält wieder z_2 noch alle Stammfactoren von v_3, v_4, ... v_n vollständig.

E. Vermöge (3. u. 4) ist weiter

$$5. \quad \frac{z}{u} = \frac{v_2 z_2}{v_2 v_3 v_4 \ldots v_n} = \frac{z_2}{v_3 v_4 \ldots v_n},$$

wo wiederum z_2 mit v_3 aufgeht.

F. Fährt man so fort, so findet sich zuletzt

$$6. \quad \frac{z}{u} = \frac{z_{n-1}}{v_n},$$

wo z_{n-1} noch alle Stammzahlen von v_n enthalten mufs und folglich mit v *aufgeht.*

Also ist $\frac{z}{u}$ nothwendig eine *ganze* Zahl; das heifst, z geht nothwendig mit dem Product $u = v_1 v_2 v_3 \ldots v_n$ auf; wie es der Lehrsatz behauptet.

G. Sind dagegen nicht alle Stammfactoren jedes v von dem jedes anderen v verschieden, so kann es sein, dafs z. B. schon bei der Division von z durch v_1 in (*B.*) Factoren von z weggenommen werden, die auch noch für ein anderes v, z. B. für v_2 nöthig sind, und folglich sind dann in (4.) *nicht* mehr nothwendig alle Stammfactoren von $v_2, v_3, v_4, \ldots v_n$ in z_1 enthalten. Mithin geht dann in diesem Fall z_1 schon nicht mehr nothwendig mit v_2 auf, und folglich auch z nicht mit u.

§. 27.

Lehrsatz.

Zwei ganze Zahlen z *und* y *können einander nicht anders gleich sein, als wenn die eine alle die Stammfactoren der andern ohne Ausnahme enthält, und auch keine mehr; so dafs also eine ganze Zahl nur auf eine einzige Art durch die Multiplication aus Stammfactoren zusammengesetzt werden kann.*

Beweis. Wenn $z = y$ sein soll, so mufs y in z und z in y *aufgehen.* Damit y in z *aufgehe,* mufs vermöge (§. 24.) z *alle* Stammfactoren von y enthalten; also keinen *weniger* als y. Und damit z in y aufgehe, mufs y *alle* Stammfactoren von z enthalten; also y keinen *weniger* als z; folglich z keinen *mehr* als y. Es mufs also z alle Stammfactoren von y enthalten, keinen *weniger* und keinen *mehr* als y, und umgekehrt. Folglich kann eine ganze Zahl nur auf eine einzige Weise ein Product von Stammfactoren sein. Andere Stammfactoren geben Zahlen, die nicht mehr in die vorige *aufgehen* und folglich auch nicht ihr gleich sein können.

§. 28.

Lehrsatz.

I. *Eine ganze Zahl ist immer gerade, das heifst, sie geht mit* 2 *auf, wenn entweder nur einer oder wenn mehrere ihrer Factoren gerade*

sind. Die Zahl kann nur dann ungerade sein, das heifst, nicht mit 2 *aufgehen, wenn kein einziger ihrer Factoren gerade ist. In diesem Falle aber ist* z *nothwendig ungerade.*

II. *Alle Stammzahlen, aufser der einzigen Stammzahl* 2, *sind ungerade Zahlen.*

III. *Jede gerade Zahl kann durch*

1. $2mn+0\pm2, \pm4, \pm6, \ldots \pm m$, *oder auch*
2. $2mn+0\pm2, \pm4, \pm6, \ldots \pm(m-1)$

ausgedrückt werden, wo n *jede beliebige Zahl und* m *in* (1.) *jede gerade, in* (2.) *jede ungerade Zahl sein kann. In* (1.) *wird durch* $2mn\pm m$ *eine und dieselbe Zahl doppelt ausgedrückt; in* (2.) *nicht.*

IV. *Jede ungerade Zahl, also auch jede Stammzahl* >2, *kann durch*

3. $2mn\pm1, \pm3, \pm5, \ldots \pm(m-1)$, *oder durch*
4. $2mn\pm1, \pm3, \pm5, \ldots \pm m$

ausgedrückt werden, wo n *jede beliebige Zahl und* m *in* (3.) *jede gerade, in* (4.) *jede ungerade Zahl sein kann. In* (4.) *wird durch* $2mn\pm m$ *eine und dieselbe Zahl doppelt ausgedrückt; in* (3.) *nicht.*

Beweis von I. *A.* Wenn einer oder mehrere Factoren der Zahl z *gerade* sind, also mit 2 aufgehen, so müssen diese Factoren unter ihren *Stammfactoren* nothwendig die Stammzahl 2 haben. Also kommt 2 unter den Stammfactoren von z ein- oder mehreremale vor. Kommt aber der Stammfactor 2 auch nur einmal vor, so geht z mit 2 auf. Also ist die Zahl z *immer* gerade, sobald nur einer oder auch mehrere ihrer Factoren gerade sind.

B. Ist kein einziger Factor von z gerade, das heifst, geht keiner derselben mit 2 auf, so kommt in keinem, und folglich auch in z selbst nicht, der Stammfactor 2 vor. Mithin geht dann, und nur dann, z mit 2 *nicht* auf und ist folglich nothwendig *ungerade.*

Beweis von II. *C.* Eine Stammzahl >2 kann deshalb keine *gerade* Zahl sein, weil sie sonst mit 2 aufgehen, folglich einen Theiler >1 haben müfste, und mithin keine Stammzahl sein würde.

Beweis von III. *D.* Dafs alle die durch (1. u. 2.) ausgedrückten Zahlen *gerade* sind, ist offenbar; denn sie gehen alle mit 2 auf.

Dafs es keine andern *geraden* Zahlen weiter gebe, als die, welche durch (1. u. 2.) ausgedrückt werden, läfst sich am kürzesten an *bestimmten* Werthen von m zeigen.

a. Es sei zuerst für *gerade m*, z. B. $m=6$, also $2m=12$, so werden *alle* gerade Zahlen 0, 2, 4, 6, 8 etc. der Reihe nach wie folgt ausgedrückt:

$$5.\quad\begin{cases} \qquad\qquad\qquad\qquad 0.12,\ 0.12+2,\ 0.12+4,\ 0.12+6, \\ 1.12-6,\ 1.12-4,\ 1.12-2,\ 1.12,\ 1.12+2,\ 1.12+4,\ 1.12+6, \\ 2.12-6,\ 2.12-4,\ 2.12-2,\ 2.12,\ 2.12+2,\ 2.12+4,\ 2.12+6, \\ 3.12-6,\ 3.12-4,\ 3.12-2,\ 3.12,\ 3.12+2,\ 3.12+4,\ 3.12+6, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Für die erste horizontale Reihe ist $n=0$, und die Zahlen, welche in dieser Reihe stehen, werden durch $2m.0+0$, 2, 4, 6 ($=m$) ausgedrückt. Für die zweite horizontale Reihe ist $n=1$, und die Zahlen, welche in dieser Reihe stehen, werden durch $2m.1\pm0$, ±2, ±4, $\pm6(=m)$ ausgedrückt. Für die dritte horizontale Reihe ist $n=2$; die Zahlen, welche in dieser Zeile stehen, werden durch $2m.2\pm0$, ±2, ±4, $\pm6(=m)$ ausgedrückt; u. s. w. Allgemein also drückt, für *irgend ein n*, $2mn\pm0$, ±2, ±4, ... $\pm m$ *jede mögliche gerade* Zahl aus. Dabei ist die *letzte* Zahl jeder Reihe *dieselbe*, wie die erste der nächstfolgenden Reihe: also drückt $2mn\pm m$ eine und dieselbe Zahl *doppelt* aus.

b. Es sei für *ungerade m*, z. B. $m=5$, also $2m=10$, so werden *alle* geraden Zahlen 0, 2, 4, 6, 8, etc. der Reihe nach wie folgt ausgedrückt:

$$6.\quad\begin{cases} \qquad\qquad\qquad 0.10,\ 0.10+2,\ 0.10+4, \\ 1.10-4,\ 1.10-2,\ 1.10,\ 1.10+2,\ 1.10+4, \\ 2.10-4,\ 2.10-2,\ 2.10,\ 2.10+2,\ 2.10+4, \\ 3.10-4,\ 3.10-2,\ 3.10,\ 3.10+2,\ 3.10+4, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Hier ist der Ausdruck der Zahlen in der ersten Zeile $0.10+0$, 2, 4 ($=m-1$), derer in der zweiten Reihe 1.10 ± 0, ±2, ±4 ($=m-1$), derer in der dritten Reihe 2.10 ± 0, ±2, ±4 ($=m-1$); und so weiter. Allgemein also drückt $2mn\pm0$, ±2, ±4, ... $\pm(m-1)$, mit irgend einem Werth von *n*, jede mögliche *gerade* Zahl aus. Dabei aber kommt, in dem gegenwärtigen Fall eines *ungeraden m*, anders wie in (5.) für ein *gerades m*, *keine* Zahl *zweimal* vor, und *keine* wird also doppelt ausgedrückt.

Dieses ist zusammen, was (III.) behauptet.

E. Auf eine ähnliche Weise läfst sich zeigen, dafs die durch (3. u. 4.) ausgedrückten Zahlen, welche offenbar alle *ungerade* sind, weil keine mit 2 aufgeht, *alle ungleichen ungeraden* Zahlen sind.

a. Es sei zuerst für *gerade m,* z. B. wieder $m=6$, also $2m=12$, so werden *alle* ungeraden Zahlen 1, 3, 5, 7, 9, ... der Reihe nach wie folgt ausgedrückt:

$$7.\quad \left\{\begin{array}{llllll} & & & 0.12+1, & 0.12+3, & 0.12+5, \\ 1.12-5, & 1.12-3, & 1.12-1, & 1.12+1, & 1.12+3, & 1.12+5, \\ 2.12-5, & 2.12-3, & 2.12-1, & 2.12+1, & 2.12+3, & 2.12+5, \\ 3.12-5, & 3.12-3, & 3.12-1, & 3.12+1, & 3.12+3, & 3.12+5, \\ \ldots & & & & & \end{array}\right.$$

Die Zahlen in der ersten horizontalen Reihe werden durch $0m+0$, 1, 3, $5\,(=m-1)$ ausgedrückt; also ist für sie $n=0$. Die Zahlen der zweiten Reihe werden durch $2m.1\pm1$, ±3, $\pm5\,(=m-1)$ ausgedrückt; also ist für sie $n=1$. Die der dritten Reihe werden durch $2m.2\pm1$, ±3, $\pm5\,(=m-1)$ ausgedrückt; also ist für sie $n=2$; und so weiter. Für *irgend einen* Werth von n drückt also $2mn\pm1$, ±3, ±5, ... $\pm(m-1)$ *jede mögliche* ungerade Zahl aus, und zwar keine zweimal; denn in (7.) ist keine der Zahlen dieselbe.

b. Für *ungerade m* sei wieder $m=5$, also $2m=10$, so werden *alle* ungerade Zahlen 1, 3, 5, 7, 9 .... wie folgt ausgedrückt:

$$8.\quad \left\{\begin{array}{llllll} & & & 0.10+1, & 0.10+3, & 0.10+5, \\ 1.10-5, & 1.10-3, & 1.10-1, & 1.10+1, & 1.10+3, & 1.10+5, \\ 2.10-5, & 2.10-3, & 2.10-1, & 2.10+1, & 2.10+3, & 2.10+5, \\ 3.10-5, & 3.10-3, & 3.10-1, & 3.10+1, & 3.10+3, & 3.10+5, \\ \ldots & & & & & \end{array}\right.$$

Die Zahlen der ersten horizontalen Reihe werden durch $2m.0+1$, 3, $5\,(=m)$ ausgedrückt, und es ist für sie $n=0$. Die Zahlen der zweiten Zeile werden durch $2m.1\pm1$, ±3, $\pm5\,(=m)$ ausgedrückt, und es ist für sie $n=1$. Die Zahlen der dritten Reihe werden durch $2m.2\pm1$, ±3, $\pm5\,(=m)$ ausgedrückt, und es ist für sie $n=2$; u. s. w. Also drückt allgemein $2mn\pm1$, ±3, ±5, ... $\pm m$ für *irgend ein n jede mögliche* ungerade Zahl aus; und zwar je die letzte in den verschiedenen Reihen *zweimal*, denn je die erste in den nächstfolgenden Reihe sind dieselben.

Dieses ist zusammen was (IV.) behauptet.

Anm. *F.* Für die *ungeraden Stammzahlen* setzt man am gewöhnlichsten $m=2$ und drückt sie also nach (3.) durch

$$9.\quad 4n\pm1$$

aus; denn mehrere Eigenschaften der durch $4n+1$ bezeichneten Stammzahlen sind, wie sich weiter unten ergeben wird, von denen der Stammzahlen $4n-1$ wesentlich verschieden.

§. 29.

Lehrsatz.

Es werde die beliebige ganze Zahl z *durch ihre Stammfactoren* a, b, c, d, ... n *ausgedrückt, nemlich nach* (§. 21.) *durch*

$$1. \quad z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu,$$

wo $\alpha, \beta, \gamma, \delta, \dots \nu$ *ganze positive Zahlen sind. Alsdann geht*

I. ***Jedes Glied der Reihe, welche das Product***

$$2. \quad P = (1+a+a^2 \dots + a^\alpha)(1+b+b^2 \dots + b^\beta)(1+c+c^2 \dots + c^\gamma) \dots$$
$$\dots (1+n+n^2 \dots + n^\nu)$$

entwickelt giebt, in z *auf. Auch hat* z ***keine andern*** *Theiler außer diesen Gliedern.*

II. *Die* ***Anzahl*** *der Theiler von* z *ist, die Einheit und* z *mit eingeschlossen,*

$$3. \quad \tau = (\alpha+1)(\beta+1)(\gamma+1) \dots (\nu+1).$$

III. *Ist* τ (3.) *eine gerade Zahl, so sind* $\frac{1}{2}\tau$ *Theiler von* z ***kleiner*** *und* $\frac{1}{2}\tau$ *Theiler* ***größer*** *als die* ***Quadratwurzel*** *aus* z. *Ist* τ ***ungerade,*** *so sind* $\frac{1}{2}(\tau-1)$ *Theiler von* z ***kleiner*** *und* $\frac{1}{2}(\tau-1)$ *Theiler* ***größer*** *als die Quadratwurzel von* z. *Die Zahl* z *ist in diesem Falle eine* ***Quadratzahl;*** *alle die Zeiger* $\alpha, \beta, \gamma, \dots \nu$ *sind dann nothwendig* ***gerade,*** *und der eine noch übrige Theiler von* z, *der durch*

$$4. \quad \sqrt{z} = a^{\frac{1}{2}\alpha} b^{\frac{1}{2}\beta} c^{\frac{1}{2}\gamma} \dots n^{\frac{1}{2}\nu}$$

ausgedrückt wird, ist die ***Quadratwurzel*** *von* z.

IV. *Die Summe aller Theiler von* z *ist*

$$5. \quad s = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \dots \frac{n^{\nu+1}-1}{n-1}.$$

Beispiel 1. Es sei

$$6. \quad z = 2^3.3^2.5 = 360,$$

also

$$7. \quad a = 2, \quad b = 3, \quad c = 5, \quad \alpha = 3, \quad \beta = 2, \quad \gamma = 1.$$

Alsdann ist nach (1.)

$$8. \quad P = (1+2+4+8)(1+3+9)(1+5),$$

und dieses giebt, entwickelt:

$$9. \quad P = 1+2+4+8+3+6+12+24+9+18+36+72+5+10+20$$
$$+40+15+30+60+120+45+90+180+360.$$

Jedes Glied dieses entwickelten Products geht in $z = 360$ auf und es giebt



keinen andern Theiler von z aufser diesen Gliedern. Die Anzahl τ der Theiler ist 24, und (3.) giebt, wie gehörig,

$$10.\quad \tau = (3+1)(2+1)(1+1) = 4.3.2 = 24.$$

τ ist hier also *gerade*. Die $\frac{1}{2}\tau = 12$ Theiler 1, 2, 4, 8, 3, 6, 12, 9, 18, 5, 10, 15 sind *kleiner* als die Quadratwurzel von z, welche zwischen 18 und 19 liegt; die übrigen $\frac{1}{2}\tau = 12$ Theiler sind *gröfser* als $\sqrt{z}$. Die *Summe* s der Theiler beträgt 1170, und wie gehörig giebt (5.)

$$11.\quad s = \frac{2^4-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1} = \frac{15}{1}\cdot\frac{26}{2}\cdot\frac{24}{4} = 15.13.6 = 1170.$$

2. Es sei

$$12.\quad z = 2^4.3^2 = 144,$$

so dafs

$$13.\quad a = 2,\quad b = 3,\quad \alpha = 4,\quad \beta = 2$$

ist, so ist in (1.)

$$14.\quad P = (1+2+4+8+16)(1+3+9),$$

und dieses giebt, entwickelt:

$$15.\quad P = 1+2+4+8+16+3+6+12+24+48+9+18+36+72+144.$$

Alle Glieder dieses entwickelten Products sind aufgehende Theiler von $z = 144$, und es giebt keine andern. Die Anzahl τ dieser Theiler ist 15, und (3.) giebt, wie gehörig,

$$16.\quad \tau = (4+1)(2+1) = 5.3 = 15.$$

τ ist *hier ungerade*. Die $\frac{1}{2}(\tau-1) = 7$ Theiler, 1, 2, 4, 8, 3, 6, 9 sind kleiner als die Quadratwurzel von z, welche 12 ist; die $\frac{1}{2}(\tau-1) = 7$ Theiler 16, 24, 48, 18, 36, 72 und 144 sind *gröfser* als die Quadratwurzel aus z. Der letzte, 15te Theiler ist 12, nemlich

$$17.\quad \sqrt{z} = 2^{\frac{4}{2}}.3^{\frac{2}{2}} = 2^2.3 = 4.3 = 12.$$

z ist hier eine *Quadratzahl*. Die *Summe* der Theiler ist 403, und wie gehörig giebt (5.)

$$18.\quad s = \frac{2^5-1}{2-1}\cdot\frac{3^3-1}{3-1} = \frac{31}{1}\cdot\frac{26}{2} = 31.13 = 403.$$

Beweis von I. *A.* z kann nicht mit *andern* Stammzahlen als a, b, c, d, ... n aufgehen (§. 14. II. u. §. 24.). Es geht aber nach (§. 14. I.) mit a, b, c, ... n und mit allen *Potenzen* von a, b, c, ... n auf, deren Zeiger nicht höher sind als α, β, γ, ... ν, und mit keinen andern; so wie mit allen *Producten* dieser Potenzen; denn alle diese sind *Factoren* von z. Es kommt daher nur darauf an, die verschiedenen möglichen Producte jener Potenzen zu finden.

B. Wäre zuerst blofs

$$19. \quad z = a^\alpha b^\beta,$$

so wären die sämmtlichen möglichen Theiler von z die Potenzen $a^0 = 1$, a^1, a^2, a^3, ... a^α von a, und $b^0 = 1$, b^1, b^2, b^3, ... b^β von b, nebst allen möglichen Producten derselben. Man findet dieselben *alle*, nemlich die *Producte* und die *Potenzen selbst*, wenn man $1 + a + a^2 \ldots\ldots + a^\alpha$ mit $1 + b + b^2 \ldots$ $\ldots + b^\beta$ *multiplicirt*. Denn zuerst 1mal $1 + a + a^2 \ldots\ldots + a^\alpha$ giebt alle Potenzen von a, welche vorkommen können. Darauf $b$mal $1 + a + a^2 \ldots\ldots + a^\alpha$ giebt alle möglichen Producte jener Potenzen mit b, so wie b selbst. b^2mal $1 + a + a^2 \ldots$ $\ldots + a^\alpha$ giebt alle möglichen Producte der vorkommenden Potenzen von a mit b^2, so wie b^2 selbst. Und so weiter. Die Multiplication von $1 + a + a^2 \ldots\ldots + a^\alpha$ mit $1 + b + b^2 \ldots\ldots + b^\beta$ giebt also alle möglichen Producte der hier vorkommenden Potenzen von a, mit allen vorkommenden Potenzen von b, und zugleich die Potenzenvon a und b selbst; also *Alles*, was gesucht wird. Mithin sind die verschiedenen Glieder des Productes $(1 + a + a^2 \ldots\ldots + a^\alpha)(1 + b + b^2 \ldots\ldots + b^\beta)$ sämmtlich Theiler von $z = a^\alpha b^\beta$ (19.) und es giebt keine anderen.

C. Es sei ferner

$$20. \quad z = a^\alpha b^\beta c^\gamma,$$

so gehen offenbar in z zunächst alle Theiler von $a^\alpha b^\beta$ auf, und keine anderen mit nur a oder b zu Stammfactoren. Sie gehen aber alle auch dann noch in z (20.) auf, wenn man sie noch mit c, mit c^2, mit c^3 u. s. w. bis c^γ multiplicirt; jedoch nicht mehr, wenn sie mit einer höheren Potenz von c als c^γ multiplicirt werden. Also findet man die sämmtlichen Theiler von z (20.), wenn man diejenigen von z (19.) mit 1, c, c^2, ... c^γ multiplicirt. Die sämmtlichen Theiler von z (19.) waren die Glieder des Products $(1 + a + a^2 \ldots\ldots + a^\alpha)$ $(1 + b + b^2 \ldots\ldots + b^\beta)$ (***B.***), also sind die Glieder des Products $(1 + a + a^2 \ldots\ldots + a^\alpha)$ $(1 + b + b^2 \ldots\ldots + b^\beta)(1 + c + c^2 \ldots\ldots + c^\gamma)$ sämmtliche Theiler von z (20.), und es giebt keine andern; denn es können keine höheren Potenzen von c vorkommen als c^γ; die Theiler 1, c, c^2, ... c^γ selbst aber, mit welchen z ebenfalls aufgeht, finden sich in dem Product durch das Glied 1, welches in $(1 + a + a^2 \ldots\ldots + a^\alpha)(1 + b + b^2 \ldots\ldots + b^\beta)$ vorkommt, ebenfalls.

D. Ganz auf ähnliche Weise folgt, dafs man, im Fall

$$21. \quad z = a^\alpha b^\beta c^\gamma d^\delta$$

ist, alle möglichen Theiler von z findet, wenn man der Reihe nach alle Theiler von z (20.) mit 1, d, d^2, ... d^δ multiplicirt, folglich, da jene Theiler nach (***C.***) die Glieder des Products $(1 + a + a^2 \ldots\ldots + a^\alpha)(1 + b + b^2 \ldots\ldots + b^\beta)$



$(1+c+c^2 \ldots\ldots + c^\gamma)$ sind, wenn man dieses Product noch mit $1+d+d^2 \ldots\ldots + d^\delta$ multiplicirt; und so weiter; so dafs also zuletzt die Glieder des Products P (2.) alle möglichen Theiler von z (1.) sind; wie es (I.) behauptet.

Beweis von II. *E.* Die *Anzahl* der Glieder des ersten Factors $1+a+a^2 \ldots\ldots + a^\alpha$ von P (2.) ist $\alpha+1$. Multiplicirt man diese Glieder mit den $\beta+1$ Gliedern des zweiten Factors $1+b+b^2 \ldots\ldots + b^\beta$, so liefert *jedes* Glied dieses zweiten Factors $\alpha+1$ Producte, also giebt die Multiplication der beiden Factoren überhaupt $(\alpha+1)(\beta+1)$ Glieder; und zwar sind alle diese Glieder unter sich *verschieden.* Denn die ersten unter sich verschiedenen $\alpha+1$ Glieder, welche aus der Multiplication von $1+a+a^2 \ldots\ldots + a^\alpha$ mit 1 entstehen, enthalten *kein* b; die zweiten $\alpha+1$ Glieder, welche aus der Multiplication von $1+a+a^2 \ldots\ldots + a^\alpha$ mit b entstehen, enthalten *sämmtlich* b, aber keine *höhere* Potenz von b; die dritten $\alpha+1$ Glieder, welche aus der Multiplication von $1+a+a^2 \ldots\ldots + a^\alpha$ mit b^2 entstehen, enthalten *sämmtlich* b^2, und keine *höhere* Potenz von b u. s. w. Also sind die $(\alpha+1)(\beta+1)$ Glieder sämmtlich von einander *verschieden.*

F. Multiplicirt man weiter die sämmtlichen $(\alpha+1)(\beta+1)$ Glieder, welche das Product $(1+a+a^2 \ldots\ldots + a^\alpha)(1+b+b^2+\ldots\ldots+b^\beta)$ enthält, und welche sämmtlich Theiler von z sind, mit den $\gamma+1$ Gliedern von $1+c+c^2 \ldots$ $\ldots + c^\gamma$, so entstehen, da jedes dieser Glieder $(\alpha+1)(\beta+1)$ Glieder liefert, zusammen $(\alpha+1)(\beta+1)(\gamma+1)$ Glieder, die alle wieder von einander *verschieden* sind, weil die ersten unter sich verschiedenen $(\alpha+1)(\beta+1)$ Glieder gar kein c, die zweiten $(\alpha+1)(\beta+1)$ von c herkommenden Glieder sämmtlich c als Factor, die dritten $(\alpha+1)(\beta+1)$ von c^2 herkommenden Glieder sämmtlich c^2 als Factor enthalten, u. s. w.

So folgt dann, wenn man weiter mit der Multiplication der Factoren von P (2.) fortfährt, dafs die *Anzahl* der Glieder dieses Products gemäfs (3.) $\tau = (\alpha+1)(\beta+1)(\gamma+1) \ldots\ldots (\nu+1)$ ist; und alle diese Glieder sind von einander verschieden. Das ist was (II.) behauptet

Beweis von III. *G.* Da z (1.) mit allen Gliedern des Products P (2.) aufgeht, so ist, wenn z_1 *irgend eines* dieser Glieder und z_2 den *Quotienten* von z dividirt durch z_1 bezeichnet,

$$22. \quad z = z_1 z_2,$$

wo z_2 eine *ganze* Zahl ist. Hieraus folgt, dafs auch der Quotient z_2 in z aufgehen und folglich nothwendig *ebenfalls eins* von den Gliedern des Products P sein mufs. Zu *jedem* Gliede des Products P gehört also nothwendig *ein*

zweites, welches, mit ihm multiplicirt, z giebt. Aber die Glieder des Products P sind ***alle*** unter sich verschieden (*F.*): also können in (22.) z_1 und z_2 einander ***nicht gleich*** sein, es wäre denn, dafs z_1 mit ***sich selbst*** multiplicirt z gäbe und also z eine ***Quadratzahl*** wäre.

Ist dies nicht der Fall, so ist nothwendig z_1 entweder ***kleiner*** oder ***gröfser*** als $\sqrt{z}$. Zu jedem $z_1 < \sqrt{z}$ gehört aber, wegen $z_1 z_2 = z$ (22.), ein $z_2 > \sqrt{z}$. Also giebt es in solchem Falle ***gerade eben so viele*** Glieder $< \sqrt{z}$ als Glieder $> \sqrt{z}$, und folglich von jeder Art $\frac{1}{2}\tau$.

Ist dagegen ***ein*** Glied vorhanden, welches, mit sich selbst multiplicirt, z giebt, so bleiben noch $\tau - 1$ Glieder ***übrig,*** und diese sind dann alle, entweder $< \sqrt{z}$ oder $> \sqrt{z}$. Von ***diesen*** $\tau - 1$ Gliedern gilt wieder dasselbe wie vorhin; und folglich sind ihrer $\frac{1}{2}(\tau - 1)$ ***kleiner*** und $\frac{1}{2}(\tau - 1)$ ***gröfser*** als $\sqrt{z}$. Das übrig bleibende ***eine*** Glied ist $= \sqrt{z}$.

H. Aber die Zahl τ der Glieder selbst ***entscheidet,*** ob ein z_1 statt finden könne, welches, ***mit sich selbst*** multiplicirt, z giebt. Ist nemlich τ ***gerade,*** so ist $\frac{1}{2}\tau$ eine ***ganze*** Zahl und folglich bleibt, da nach (*G.*) $\frac{1}{2}\tau$ Glieder kleiner und $\frac{1}{2}\tau$ Glieder gröfser als $\sqrt{z}$ sein müssen, ***kein*** Glied ***übrig,*** welches ***gleich*** $\sqrt{z}$ sein könnte. Die Zahl τ (3.) ist aber nach (§. 28. I.) ***immer gerade,*** wenn auch nur ein einziger ihrer Factoren $\alpha+1$, $\beta+1$, $\gamma+1$, ... $\nu+1$ ***gerade,*** also nur ein einziger der Exponenten α, β, γ, ... ν ***ungerade*** ist. In solchem Falle also giebt es keine Quadratwurzel aus z, die eine ganze Zahl wäre.

Ist dagegen τ ***ungerade,*** so ist $\frac{1}{2}(\tau - 1)$ eine ***ganze*** Zahl, und da alsdann $\frac{1}{2}(\tau - 1)$ Glieder ***kleiner*** und $\frac{1}{2}(\tau - 1)$ Glieder ***gröfser*** als $\sqrt{z}$ sind (*G.*), so bleibt ***ein Glied*** übrig, welches, mit sich selbst multiplicirt, z giebt. Es ist aber τ nach (§. 28. I.) nur dann ***ungerade,*** wenn ***keiner*** der Factoren $\alpha+1$ $\beta+1$, $\gamma+1$, ... $\nu+1$ ***gerade,*** also wenn ***keiner*** der Exponenten α, β, γ, ... ν ***ungerade*** ist. Also ***nur*** in diesem Fall giebt es eine ganzzahlige Quadratwurzel von z. Dieses zusammen ist was (III.) behauptet.

Beweis von IV. ***I.*** Die Summe der sämmtlichen Glieder des entwickelten Products P (2.) ist der ***Werth*** des Products selbst. Nun ist

$$23. \quad 1 + a + a^2 + a^3 \ldots\ldots + a^\alpha = \frac{a^{\alpha+1} - 1}{a - 1};$$

denn multiplicirt man hier rechts und links mit $a - 1$, so ergiebt sich

$$24. \quad \left\{ \begin{array}{l} \quad\;\; a + a^2 + a^3 + a^4 \ldots\ldots + a^\alpha + a^{\alpha+1} = a^{\alpha+1} - 1, \\ -1 - a - a^2 - a^3 - a^4 \ldots\ldots - a^\alpha \end{array} \right.$$

wie gehörig. Eben so ist $1+b+b^2 \ldots\ldots +b^\beta = \frac{b^{\beta+1}-1}{b-1}$, $1+c+c^2 \ldots\ldots c^\gamma = \frac{c^{\gamma+1}-1}{c-1}$, u. s. w. Also läfst sich P, dessen *Werth* in (5.) durch s bezeichnet wurde, wie folgt ausdrücken:

$$25. \quad s = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \ldots\ldots \frac{n^{\nu+1}-1}{n-1};$$

wie (IV.) es behauptet.

Anm. Die Hauptmomente in dem Beweise sind, dafs der Ausdruck (1) von z mit keinen *höheren* Potenzen von $a, b, c, \ldots\ldots n$ aufgeht, als mit denen, deren Exponenten $\alpha, \beta, \gamma, \ldots\ldots \nu$ sind; sodann, dafs alle diese Potenzen in den Gliedern des Products P (2.) vorkommen; und endlich, dafs alle Glieder des Products P von einander *verschieden* sind.

§. 30.

Lehrsatz.

Jede Menge von Einheiten, also jede ganze Zahl z, *kann, wenn* a *eine beliebige andere, kleinere Menge von Einheiten bezeichnet, durch*

$$1. \quad z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + x_{m-3} a^{m-3} \ldots\ldots + x_1 a + x_0$$

ausgedrückt werden, wo die x *sämmtlich ganze Zahlen und sämmtlich kleiner als* a *sind.* m *ist ebenfalls eine ganze Zahl, deren Gröfse sich nach* z *und* a *richtet. Die* x *können für ein- und dasselbe* z *und* a *jedes nur einen Werth haben. Bestimmt man für die verschiedenen Werthe, welche die* x *haben können, und deren* a — 1 *sind, ausschliefsliche, willkürliche Zeichen, und dann noch für Null ebenfalls ein Zeichen, so kann* z *durch diese Zeichen, blofs der Reihe nach hinter einander geschrieben, ausgedrückt werden, ohne* a *selbst zu schreiben. Dieses Mittel Mengen von Einheiten auszudrücken, giebt die Zahlensysteme. Die Zeichen für die verschiedenen möglichen Werthe von* x *sind die Ziffern, und die verschiedenen Potenzen von* a *werden als eben so viele verschiedene Einheiten betrachtet, deren Werthe die Stellen der Ziffern schon ausdrücken. In dem üblichen dekadischen Zahlensystem enthält* a *zehn Einheiten, und die* a — 1 *Ziffern* 1, 2, 3, 4, 5, 6, 7, 8 und 9, *nebst dem Zeichen* 0 *für Null, reichen hin, jede Menge* z *von Einheiten, also jede ganze Zahl auszudrücken.*

Beweis. *A.* Welche Menge von Einheiten auch z enthalten mag: es wird immer durch wiederholte Multiplication von a mit sich selbst, sobald

a mehr als *eine* Einheit enthält, zu einer Zahl a^m zu gelangen sein, die, wenn man sie *noch einmal* mit a multiplicirt, eine Zahl giebt, welche *gröfser* ist als z. Denn durch wiederholte Multiplication mit a kann man die Menge der Einheiten in dem Product bis *in's Unendliche* vergröfsern.

B. Ist nun a^m diejenige Potenz von a, welche noch *kleiner* als z ist, aber, noch einmal mit a multiplicirt, eine Zahl giebt, die *gröfser* ist als z, so wird sich z durch

$$2. \quad z = x_m a^m + r_1$$

ausdrücken lassen, wo $x_m < a$ und $r_1 < a^m$ ist. Denn wäre x_m gleich a oder $> a$, so wäre $x_m a^m + r_1$ gleich $a^{m+1} + r_1$, also *gröfser* als z, gegen die Voraussetzung; r_1 aber kann immer $< a^m$ gemacht werden, da man nur a^m so oft von z abziehen darf, als es möglich ist.

C. Da also $r_1 < a^m$ ist, aber möglicherweise $> a^{m-1}$ sein kann, so wird sich aus gleichen Gründen r_1 wieder wie folgt ausdrücken lassen:

$$3. \quad r_1 = x_{m-1} a^{m-1} + r_2,$$

wo wieder x_{m-1} nothwendig $< a$ und $r_2 < a^{m-1}$ ist. Eben so wird weiter

$$4. \quad \begin{cases} r_2 = x_{m-2} a^{m-2} + r_3, \\ r_3 = x_{m-3} a^{m-3} + r_4, \\ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \end{cases}$$

gesetzt werden können, bis man zuletzt auf ein r kommt, welches kleiner als a selbst ist und folglich in die Reihe der x gehört, die *alle* $< a$ sind.

D. Substituirt man die Ausdrücke (2., 3. u. 4.) in einander, so ergiebt sich der Reihe nach

$$5. \quad \begin{cases} z = x_m a^m + r_1, \\ z = x_m a^m + x_{m-1} a^{m-1} + r_2, \\ z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + r_3, \\ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + x_{m-3} a^{m-3} \; \ldots \; + x_1 a + x_0. \end{cases}$$

Der letzte dieser Ausdrücke von z ist der (1.) des Lehrsatzes.

E. Bestimmt man nun für die $a-1$ verschiedenen Werthe, welche x haben kann, eben so viele ausschliefsliche, verschiedene Zeichen oder *Ziffern*, z. B. für das dekadische System die Ziffern 1, 2, 3, 4, 5, 6, 7, 8, und 9 und für Null das Zeichen 0, so kann zunächst *a selbst* blofs durch 10 bezeichnet werden; denn für $z = a$ sind in (1.) *alle* x, mit Ausnahme von x_1, gleich Null; x_m aber ist $= 1$. Also ist z oder $x_1 a + x_0$ hier $1 . x + 0 . 1$, und wenn man nun x selbst als eine neue Einheit betrachtet, welche zehn

der einfachen Einheiten enthält, so kann man blofs schreiben $1.1+0.1$, oder zusammengezogen 10, wo schon die *Stelle* der 1 ausdrückt, dafs die *nächst höhere* Einheit gemeint sei.

Eben so sind für $z=a^2$ *alle* x, mit Ausnahme von x_2, gleich Null, und x_2 ist $=1$. Also ist $z=x_{m-1}a^2+0.1+0=1.1+0.1+0$, wofür zusammengezogen blofs 100 geschrieben werden kann, da die Stelle der 1 schon anzeigt, welche Potenz von a gemeint sei. Und so weiter.

Sind nun die verschiedenen x *nicht* Null, so multipliciren sie der Reihe nach die verschiedenen Einheiten oder Potenzen von a, deren Exponenten schon von den Stellen der Ziffern angezeigt werden; denn keine Ziffer, da sie nur ein einziges Zeichen ist, nimmt mehr als eine Stelle ein.

Also läfst sich jede Menge z von Einheiten blofs durch die hinter einander geschriebenen Ziffern oder Mengen der verschiedenen Potenzen von a ausdrücken.

F. Um zu zeigen, dafs für ein- und dasselbe z und a, die x jedes *nur einen* Werth haben können, setze man, es könne ein- und dasselbe z, aufser wie in (1.), auch durch

$$6.\quad z=y_m a^m+y_{m-1}a^{m-1}+y_{m-2}a^{m-2}\ \ldots\ +y_1 a+y_0$$

ausgedrückt werden, wo die y von den x in (1.) *verschieden* sind.

Man ziehe (6.) von (1.) ab, so ergiebt sich

$$7.\quad 0=(x_m-y_m)a^m+(x_{m-1}-y_{m-1})a^{m-1}+(x_{m-2}-y_{m-2})a^{m-2}\ \ldots$$
$$\ldots+(x_1-y_1)a^1+x_0-y_0.$$

In diesem Ausdruck geht rechterhand Alles bis auf x_0-y_0 mit a auf, also mufs nach (§. 18.) auch x_0-y_0 mit a aufgehen. Dies aber ist nicht anders möglich, als wenn x_0-y_0 gleich *Null* ist, da x_0 und y^0 beide nach der Voraussetzung $<a$ sind und also auch $x_0-y_0<a$ ist. Also mufs nothwendig y_0 *gleich* x_0 sein.

Läfst man x_0-y_0, als Null, aus (7.) weg und dividirt was übrig bleibt durch a, so ergiebt sich

$$8.\quad 0=(x_m-y_m)a^{m-1}+(x_{m-1}-y_{m-1})a^{m-2}+(x_{m-2}-y_{m-2})a^{m-3}\ \ldots$$
$$\ldots+(x_2-y_2)a_2+x_1-y_1,$$

und hieraus folgt, ganz aus demselben Grunde wie vorhin, dafs auch y_1 *gleich* x_1 sein mufs.

Läfst man wieder x_1-y_1, als Null, aus (8.) weg und dividirt was übrig bleibt durch a, so folgt ferner, dafs auch y_2 *gleich* x_2 sein mufs. Und so weiter für alle x und y bis zu $y_m=x_m$ selbst. Also können für ein- und dasselbe z und a die x in (1.) jedes *nur einen* Werth haben.

§. 31.

Lehrsatz.

I. ***Jede ganze Zahl ist die Summe dieser oder jener Potenzen der Zahl*** 2; ***und zwar nur auf eine Art.***

II. ***Jede ganze Zahl ist die Summe dieser oder jener Potenzen der Zahl*** 3, ***weniger der Summe dieser oder jener Potenzen derselben Zahl*** 3; ***und zwar wieder nur auf eine Art.***

Beispiel zu I. Es ist $83 = 64 + 16 + 2 + 1 = 2^6 + 2^4 + 2^1 + 2^0$; $74 = 64 + 8 + 2 = 2^6 + 2^3 + 2^1$; $181 = 128 + 32 + 16 + 4 + 1 = 2^7 + 2^5 + 2^4 + 2^2 + 2^0$ u. s. w.

Zu II. Es ist $83 = 81 + 3 - 1 = 3^4 + 3^1 - 3^0$; $74 = 81 - 9 + 3 - 1 = 3^4 - 3^2 + 3^1 - 3^0$; $181 = 243 - 81 + 27 - 9 + 1 = 3^5 - 3^4 + 3^3 - 3^2 + 3^0$.

Beweis von I. *A.* Nach (§. 30.) kann *jede* ganze Zahl durch

$$1. \quad z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} \ldots . + x_1 a + x_0$$

ausgedrückt werden, wo a *willkürlich* ist und *alle* $x < a$ sind.

Setzt man also das *willkürliche* $a = 2$, so können die x nur 1 oder 0 sein. Also wird jede Zahl z durch

$$2. \quad z = x_m 2^m + x_{m-1} 2^{m-1} + x_{m-2} 2^{m-2} \ldots . x_1 2 + x_0$$

ausgedrückt, wo die x *nie gröfser* als 1, jedoch diese oder jene x auch Null sein können. Also wird jedes z blofs durch *einmal* genommene Potenzen von $a = 2$ ausgedrückt, unter welchen diese oder jene *fehlen* können. Jedes z ist also die Summe dieser oder jener Potenzen (nemlich derer, die *nicht* fehlen) von der Zahl $a = 2$.

B. Ferner können für ein- und dasselbe z und a die x (2.) nach (§. 30.) jedes *nur einen* Werth haben: also kann auch hier z *nur auf eine Art* aus diesen oder jenen Potenzen von 2 zusammengesetzt werden.

Beweis von II. *C.* Setzt man in (1.) $a = 3$, so können die x, weil sie $< a$ sein sollen, nur 0, 1 oder 2 sein. Diejenigen, welche 0 oder 1 sind, geben die Potenzen von $a = 3$ entweder gar nicht, oder blofs einmal. Für diejenigen, welche 2 sein müssen, setze man $2 = 3 - 1 = a - 1$. Dadurch geht das Glied, welches 2 zum Coëfficienten hat, mit einem seiner Theile in die nächst höhere Potenz von a, also zu dem nächstvorhandenen Gliede über, der andere Theil aber kommt dann nur einfach, und zwar negativ vor. Z. B. wenn zwei aufeinander folgende Glieder in (1.) $x_k 3^k + 2.3^{k-1}$ wären, so verwandeln sie sich, wenn man $3 - 1$ statt 2 schreibt, in

$x_k.3^k + 3.3^{k-1} - 3^{k-1} = x_k.3^k + 3^k - 3^{k-1} = (x_k+1)3^k - 3^{k-1}$. Ist hier x_k nicht 0, sondern 1, so bekommt 3^k zum Coëfficienten 2 und man kann wie vorhin verfahren. Ist x_k schon 2, so kann man zuvor schon statt dessen $3-1$ statt 2 setzen, u. s. w., falls es nöthig ist, bis zum *ersten* Gliede $x_m a^m$ hinauf, welches, wenn $x_m = 2$ wäre, $3.a^m - a^m = a^{m+1} - a^m$ geben würde. Also lassen sich überall die Coëfficienten 2, wo sie vorkommen, wegschaffen, und es lassen sich die x blofs auf $+1$, -1 und 0 reduciren, also so, dafs z blofs durch eine Summe dieser oder jener Potenzen der Zahl 3, *weniger* der Summe dieser oder jener andern Potenzen derselben Zahl 3 ausgedrückt wird.

D. Dafs solches *nur auf eine Art* geschehen kann, folgt daraus, dafs in (2.) die x nach (§. 30.) allgemein für ein- und dasselbe a und z jedes *nur einen Werth* haben können.

§. 32.

Lehrsatz.

Wenn man eine beliebige gegebene ganze Zahl Z *nach* (§. 30. 1.) *durch*

$$1. \quad Z = x_m A^m + x_{m-1} A^{m-1} + x_{m-2} A^{m-2} \ldots + x_2 A^2 + x_1 A + x_0$$

ausdrückt, und man setzt

$$2. \quad nA = \mathfrak{G}s + r,$$

wo s *ebenfalls gegeben,* n *willkürlich aber zu* s *theilerfremd und* $r < s$ *ist, so geht* Z (1.) *mit der Zahl* s *auf, oder nicht auf, je nachdem*

$$3. \quad z = x_m r^m + n x_{m-1} r^{m-1} + n^2 x_{m-2} r^{m-2} + n^3 x_{m-3} r^{m-3} \ldots \\ \ldots + n^{m-2} x_2 r^2 + n^{m-1} x_1 r + n^m x_0$$

mit s *aufgeht, oder nicht aufgeht.*

Beweis. *A.* Wenn man von (2.) z. B. die *k*te Potenz nimmt, so ist nach (§. 11. No. 5.)

$$4. \quad n^k A^k = \mathfrak{G}s + r^k;$$

also der Reihe nach

$$5. \quad \begin{cases} nA = \mathfrak{G}s + r, \\ n^2 A^2 = \mathfrak{G}s + r^2, \\ n^3 A^3 = \mathfrak{G}s + r^3, \\ n^4 A^4 = \mathfrak{G}s + r^4, \\ \ldots\ldots\ldots\ldots \\ n^m A^m = \mathfrak{G}s + r^m. \end{cases}$$

B. Nun multiplicire man (1.) mit n^m, so ergiebt sich

$$6. \quad n^m Z = x_m n^m A^m + x_{m-1} n^m A^{m-1} + x_{m-2} n^m A^{m-2} \ldots \ldots + x_2 n^m A^2 + x_1 n^m A + x_0 n^m.$$

Setzt man hierin die Ausdrücke von nA, n^2A^2, n^3A^3, ..., so erhält man

$$\begin{aligned} 7. \quad n^m Z = & \; x_m \; (\mathfrak{S}s + r^m) \\ & + x_{m-1}(\mathfrak{S}s + r^{m-1})n \\ & + x_{m-2}(\mathfrak{S}s + r^{m-2})n^2 \\ & + x_{m-3}(\mathfrak{S}s + r^{m-3})n^3 \\ & \ldots\ldots\ldots\ldots \\ & + x_2 \; (\mathfrak{S}s + r^2) \; n^{m-2} \\ & + x_1 \; (\mathfrak{S}s + r) \; n^{m-1} \\ & + x_0 \; n^m, \end{aligned}$$

oder, nach (§. 11.),

$$8. \quad n^m Z = \mathfrak{S}s + x_m r^m + n x_{m-1} r^{m-1} + n^2 x_{m-2} r^{m-2} \ldots \ldots + n^{m-2} x_2 r^2 + n^{m-1} x_1 r + n^m x_0,$$

oder auch, durch (3.) ausgedrückt,

$$9. \quad n^m Z = \mathfrak{S}s + z.$$

C. Geht nun hier z mit s auf, so gehen die ***beiden*** Glieder $\mathfrak{S}s$ und z mit s auf. Also mufs alsdann nach (§. 18.) auch das ***dritte*** Glied $n^m.Z$ mit s aufgehen. Aber n ist nach der Voraussetzung zu s ***theilerfremd***, also auch n^m. Mithin geht von den beiden Factoren n^m und Z der Factor n^m ***nicht*** mit s auf. Dieserhalb mufs zufolge (§. 25. I.) nothwendig der ***andere*** Factor Z mit s aufgehen. Also folgt, dafs, wenn z (3.) mit s ***aufgeht***, auch Z (1.) mit s ***aufgehen*** mufs.

D. Geht in (9.) z ***nicht*** mit s auf, so kann auch Z nicht mit s aufgehen, denn sonst wäre $\frac{n^m Z}{s}$, so wie $\frac{\mathfrak{S}s}{s} = \mathfrak{S}$, eine ganze Zahl, also auch in $\frac{n^m Z - \mathfrak{S}s}{s} = \frac{z}{s}$, $\frac{n^m Z - \mathfrak{S}s}{s}$ eine ganze Zahl, $\frac{z}{s}$ dagegen ein Bruch, und einer ganzen Zahl kann ein Bruch nicht gleich sein

Dieses zusammen ist was der Lehrsatz behauptet.

Anm. Der Beweis beruht auf (§. 11, 18. und 25. I.).

§. 33.

Aufgabe.

Ob eine gegebene ganze Zahl Z mit einer andern gegebenen Zahl s ***aufgehe***, vermittels anderer, von Z und s abhängender Zahlen z zu finden.

die, während sie *kleiner* sind als Z, die Eigenschaft haben, dafs, je nachdem sie mit s aufgehen oder nicht aufgehen, das Gleiche auch mit Z geschieht.

Auflösung. *A.* In (§. 32.) zeigte sich, dafs

$$1.\quad Z = x_m A^m + x_{m-1} A^{m-1} + x_{m-2} A^{m-2} \;\ldots\; + x_2 A^2 + x_1 A + x_0$$

mit s *aufgeht*, oder nicht *aufgeht*, je nachdem die Zahl

$$2.\quad z = x_m r^m + x_{m-1} n r^{m-1} + x_{m-2} n^2 r^{m-2} + x_{m-2} n^3 r^{m-3} \ldots$$
$$\ldots + x_2 n^{m-2} r^2 + x_1 n^{m-1} r + x_0 n^m,$$

in deren Ausdruck

$$3.\quad nA = \mathfrak{G}s + r$$

n eine *willkürliche* zu s *theilerfremde* Zahl ist, mit s *aufgeht* oder *nicht aufgeht.*

B. Dieser Satz kann zur Auflösung der gegenwärtigen Aufgabe dienen. Denn da r in (3.), wenn man es den *echten* positiven oder negativen Rest zu s sein läfst, jedenfalls $< s$, und wenn man für r den *unbedingt echten* Rest zu s nimmt, sogar $< \frac{1}{2}s$ ist, und man von den Multiplicatoren der x in (2.) wiederum nur die echten Reste zu s zu nehmen braucht: so sind die Multiplicatoren der x in (2.) immer kleiner als in (1.), und folglich ist immer z kleiner als Z. Der Ausdruck (1.) für Z aber drückt nach (§. 30.) jede beliebige Zahl aus, und es ist nicht nöthig, dafs man grade, wie im dekadischen System, $A = 10$ setzt, sondern es kann für A willkürlich eben sowohl $10^2 = 100$, $10^3 = 1000$ und so weiter genommen werden. Setzt man $A = 10$, so sind die x blofs einfache Ziffern < 10. Setzt man $A = 100$, so sind die x Zahlen von 2 Ziffern und < 100. Überhaupt sind die x, wenn man $A = 10^k$ setzt, Zahlen von k Ziffern, aber jedenfalls $< A$. Für das dekadische Zahlensystem heifst die Gleichung (3.) allgemein

$$4.\quad n.10^k = \mathfrak{G}s + r,$$

und in dieser Gleichung sind die *beiden* Zahlen k und n *willkürlich.*

C. Da nun z (2.) *um so kleiner* sein wird, je kleiner r und n sind, insofern nicht k wiederum die x sehr grofs macht, so wird man die willkürlichen n und k so anzunehmen suchen müssen, dafs die r und n möglichst klein sind. Am *vortheilhaftesten* ist es offenbar, wenn r und n beide $= 1$ sein können; und *gut*, wenn wenigstens eins von ihnen $= 1$ ist.

D. Wenn s eine *theilbare* Zahl ist, so darf man eigentlich nur untersuchen, ob diejenigen *Stammzahlen*, oder diejenigen Potenzen von *Stammzahlen*, welche die Factoren von s sind, in Z aufgehen oder nicht. Denn wenn alle diese Factoren in Z aufgehen, so geht auch s in Z auf (§. 26.). Doch hindert nichts, auch s *auf einmal* in Rechnung zu bringen, wenn man

nur für n Zahlen setzt, die mit s keinen Theiler gemein haben. Vor Allem kommt es indessen auf die *Stammzahlen* an.

E. Auch kann, wenn ja z noch eine sehr *grofse* Zahl ist, auf dieselbe das Verfahren *wiederholt angewendet werden*, um zu noch *kleineren* Zahlen zu gelangen, mit welchen *zugleich* Z mit s aufgehe oder nicht aufgehe.

Beispiele.

No. 1. Es sei

$$s = 3 \quad \text{und} \quad s = 3^2 = 9.$$

Für diese beiden Werthe von s ist schon

$$5. \quad 10 = \mathfrak{G}.3+1 = \mathfrak{G}.9+1;$$

also $n=1$, $k=1$, $r=1$ und in (2.)

$$6. \quad z = x_0+x_1+x_2 \ldots\ldots +x_m,$$

wo, wegen $k=1$, die x die *blofsen Ziffern* von Z sind. Also geht die Zahl Z mit 3 und 9 auf, wenn die *Summe ihrer Ziffern* mit 3 und 9 aufgeht; wie bekannt.

No. 2. Es sei

$$s = 27 = 3^3.$$

Hier ist

$$7. \quad 10^3 = 37.27+1 = \mathfrak{G}.27+1;$$

also ist hier $n=1$, $k=3$ und $r=1$, und folglich in (2.) wieder

$$8. \quad z = x_0+x_1+x_2 \ldots\ldots +x_m,$$

wo aber, wegen $k=3$, die x die Zahlen sind, welche je *drei Ziffern* von Z von der Rechten zur Linken ausdrücken. Folglich geht Z mit 27 auf, wenn die *Summe jener Zahlen* x mit 27 aufgeht.

Wäre z. B.

$$9. \quad Z = 25084365147,$$

so wäre

$$10. \quad z = 147+365+84+25 = 621.$$

Dieses z geht mit 27 auf, also mufs auch Z mit 27 aufgehen; was auch der Fall ist.

No. 3. Es sei

$$s = 81 = 3^4.$$

Hier ist

$$11. \quad 10^9 = 12345679.81+1 = \mathfrak{G}.81+1,$$

also ist hier $n=1$, $k=9$, $r=1$ und in (2.) wieder

$$12. \quad z = x_0+x_1+x_2 \ldots\ldots +x_m,$$

wo, wegen $k=9$, die x die Zahlen sind, welche je *neun* Ziffern von Z

von der Rechten zur Linken ausdrücken, und Z geht mit 81 auf, wenn die *Summe* dieser Zahlen mit 81 aufgeht.

Da aber z hier schon wenigstens 9 Ziffern hat, und also sehr grofs ist, so mag man (4.) anders anzuwenden versuchen.

Es ist

$$13.\quad 8.10 = \mathfrak{G}.81-1,$$

also $n=8$, $k=1$, $r=-1$. Dieses giebt zunächst in (2.)

$$14.\quad z = (-1)^m[x_m - nx_{m-1} + n^2x_{m-2} - n^3x_{m-3} \dots \pm n^{m-1}x_1 \mp n^m x_0].$$

Sodann ist (nach §. 11. Anm. gerechnet, nemlich die echten Reste ϱ der Multiplicatoren der x genommen):

$$15.\quad \begin{cases} n = 8, & \text{also } \varrho_m = +8, \\ n^2 = \mathfrak{G}.81-17, & \text{also } \varrho_{m-1} = -17, \\ n^3 = \mathfrak{G}.81+26, & \text{also } \varrho_{m-2} = +26, \\ n^4 = \mathfrak{G}.81-35, & \text{also } \varrho_{m-3} = -35, \\ n^5 = \mathfrak{G}.81-37, & \text{also } \varrho_{m-4} = -37, \\ n^6 = \mathfrak{G}.81+28, & \text{also } \varrho_{m-5} = +28, \\ n^7 = \mathfrak{G}.81-19, & \text{also } \varrho_{m-6} = -19, \\ n^8 = \mathfrak{G}.81+10, & \text{also } \varrho_{m-7} = +10, \\ n^9 = \mathfrak{G}.81-\ \,1, & \text{also } \varrho_{m-8} = -\ \,1; \end{cases}$$

(Die folgenden ϱ sind wieder dieselben; nur haben sie entgegengesetzte Zeichen.)

folglich ist in (14.)

$$16.\quad z = \pm[x_m - 8.x_{m-1} - 17.x_{m-2} - 26.x_{m-3} - 35.x_{m-4} + 37.x_{m-5} \\ + 28.x_{m-6} + 19.x_{m-7} + 10.x_{m-8} + \dots],$$

wo die x die blofsen Ziffern der Zahl Z von der Linken zur Rechten sind.

Wäre z. B.

$$17.\quad Z = 7943949936972,$$

so wäre nach (16.)

$$z = \pm[7-8.9-17.4-26.3-35.9+37.4+28.9+19.9+10.3 \\ +1.6-8.9-17.7-26.2] \text{ oder}$$

$$18.\quad z = \pm[7-72-68-78-315+148+252+171+30+6-72-119-52] \\ = \pm(614-776) = \mp 162.$$

Dieses z geht mit 81 auf, also mufs auch Z (17.) mit 81 aufgehen; was auch der Fall ist.

No. 4. Es sei

$$s = 7.$$

Hier ist

$$19.\quad 10^3 = 143.7-1,$$

also $n=1$, $k=3$ und $r=1$ und in (2.)

$$20.\quad z = x_0 - x_1 + x_2 - x_3 \ldots\ldots \pm x_m,$$

wo die x die 3ziffrigen Zahlen in Z von der Rechten zur Linken sind.

Wäre z. B.

$$21.\quad Z = 80939417280533,$$

so wäre zufolge (20.)

$$22.\quad z = 533 - 280 + 417 - 939 + 80 = 1030 - 1219 = -189.$$

Dieses z geht mit 7 auf; also auch Z.

Wollte man (4.) anwenden, so könnte man setzen

$$23.\quad 5.10 = \mathfrak{G}.7 + 1;$$

also wäre $n=5$, $k=1$ und $r=1$. Dieses giebt für z in (2.)

$$24.\quad z = x_m + n x_{m-1} + n^2 x_{m-2} + n^3 x_{m-3} \ldots\ldots + n^m x_0.$$

Nun ist

$$25.\quad \begin{cases} n = \mathfrak{G}.7-2, & n^4 = \mathfrak{G}.7+2, & n^7 = \mathfrak{G}.7-2, \\ n^2 = \mathfrak{G}.7-3, & n^5 = \mathfrak{G}.7+3, & n^8 = \mathfrak{G}.7-3, \quad \text{u. s. w.} \\ n^3 = \mathfrak{G}.7-1, & n^6 = \mathfrak{G}.7+1, & n^9 = \mathfrak{G}.7-1, \end{cases}$$

also in (24.)

$$z = x_m - 2x_{m-1} - 3x_{m-2} - x_{m-3} + 2x_{m-4} + 3x_{m-5} + x_{m-6} \ldots\ldots \text{ oder}$$

$$26.\quad z = x_m - x_{m-3} + x_{m-6} - x_{m-9} \ldots\ldots - 2(x_{m-1} - x_{m-4} + x_{m-7} \ldots\ldots) - 3(x_{m-2} - x_{m-5} + x_{m-8} \ldots\ldots),$$

wo die x die einfachen Ziffern von Z sind. Dieser Ausdruck giebt z. B. für die Zahl Z (21.)

$$z = 8-3+1-8+3-2(0-9+7-0+3)-3(9-4+2-5) \text{ oder}$$

$$27.\quad z = +1-2(+1)-3(+2) = +1-2-6 = -7.$$

Dieses z geht mit 7 auf; also auch Z.

No. 5. Es sei

$$s = 11.$$

Hier ist

$$28.\quad 10 = \mathfrak{G}.11 - 1 \quad \text{und} \quad 10^2 = \mathfrak{G}.11 + 1,$$

also $n=1$ und $r=-1$ für $k=1$, $r=+1$ für $k=2$. Mithin giebt (2.)

$$29.\quad z = -x_m + x_{m-1} - x_{m-2} + x_{m-3} \ldots\ldots,$$

wo die x die einfachen Ziffern von Z sind, und

$$30.\quad z = x_m + x_{m-1} + x_{m-2} + x_{m-3} \ldots\ldots,$$

wo die x die *zweiziffrigen* Zahlen in Z von der Rechten zur Linken bedeuten.

Z. B. für

$$31.\quad Z = 37201458690434819$$

giebt (29.)

32. $z = -3+7-2+0-1+4-5+8-6+9-0+4-3+4-8+1-9$
$= -37+37 = 0$

und (30.) giebt

33. $z = 19+48+43+90+86+45+1+72+3 = 407$

und, *wiederholt* angewendet,

34. $z = 4+7 = 11.$

Diese z gehen mit 11 auf; also geht auch Z (31.) mit 11 auf.

No. 6. Es sei

$$s = 13.$$

Hier ist

35. $10^3 = 77.13-1 = \mathfrak{G}.13-1,$

also $n=1$, $k=3$, $r=-1$, mithin nach (2.)

36. $z = x_0 - x_1 + x_2 - x_3 \ldots \pm x_m,$

wo die x die *dreizifrigen* Zahlen in Z von der Rechten zur Linken sind; eben wie in No. 4. für $s=7$.

Will man (4.) anwenden, so kann man setzen:

37. $4.10 = \mathfrak{G}13+1,$

also $n=4$, $k=1$, $r=+1$, folglich in (2.)

38. $z = x_m + 4x_{m-1} + 4^2.x_{m-2} + 4^3.x_{m-3} \ldots,$

und da

39. $\begin{cases} n = \mathfrak{G}s+4, & n^4 = \mathfrak{G}s-4, & n^7 = \mathfrak{G}s+4, \\ n^2 = \mathfrak{G}s+3, & n^5 = \mathfrak{G}s-3, & n^8 = \mathfrak{G}s+3, \\ n^3 = \mathfrak{G}s-1, & n^6 = \mathfrak{G}s+1, & n^9 = \mathfrak{G}s-1, \end{cases}$ u. s. w.

ist,

$z = x_m + 4x_{m-1} + 3x_{m-2} - x_{m-3} - 4x_{m-4} - 3x_{m-5} \ldots$ oder

40. $z = (x_m - x_{m-3} + x_{m-6} - x_{m-9} \ldots) + 4(x_{m-1} - x_{m-4} + x_{m-7} \ldots)$
$+3(x_{m-2} - x_{m-5} + x_{m-8} \ldots),$

wo die x die einfachen Ziffern von Z sind.

Wäre z. B.

41. $Z = 5891476201146758014,$

so würde (36.)

42. $z = 14-758+146-201+476-891+5 = 641-1850 = -1209$

und, *wiederholt* angewendet,

43. $z = 209-1 = 208$

geben. Hingegen (40.) würde geben:

$$z = 5-1+6-1+6-8+4+4(8-4+2-1+7-0)$$
$$+3(9-7+0-4+5-1) \text{ oder}$$

44. $z = 21-10+4(17-5)+3(14-12) = 11+48+6 = 65.$

Die z (43. und 44.) gehen mit $s = 13$ auf; also auch Z (41.).

No. 7. Es sei

$$s = 17.$$

Hier kann man setzen:

45. $10^2 = \mathfrak{G}.17-2,$

also

46. $n = 1, \quad k = 2, \quad r = -2.$

Dieses giebt in (2.)

$$z = x_0 - 2x_1 + 2^2.x_2 - 2^3 x_3 + 2^4 x_4 \ldots. \text{ oder}$$
$$z = x_0 - 2x_1 + 4x_2 - 8x_3 - x_4 + 2x_5 - 4x_6 + 8x_7 + x_8 \ldots. \text{ oder}$$

47. $z = (x_0 - x_4 + x_8 - x_{12} \ldots.) - 2(x_1 - x_5 + x_9 \ldots.) + 4(x_2 - x_6 + x_{10} \ldots.)$
$- 8(x_3 - x_7 + x_{11} \ldots.),$

wo die x die *zweiziffrigen* Zahlen in Z von der Rechten zur Linken sind.

Setzt man dagegen in (4.) $n = 5$, $k = 1$, so erhält man

48. $5.10 = \mathfrak{G}.17-1$ also $r = -1.$

Dieses giebt in (2.)

$$z = -x_m + 5x_{m-1} - 5^2 x_{m-2} + 5^3 x_{m-3} - 5^4 x_{m-4} \ldots. \text{ oder}$$

49. $z = -x_m + 5x_{m-1} - 8x_{m-2} + 6x_{m-3} + 4x_{m-4} - 3x_{m-4} + 2x_{m-5}$
$- 7x_{m-6} - x_{m-7} + 5x_{m-8} \ldots.,$

wo x die einfachen Ziffern von Z sind.

Es sei z. B.

50. $Z = 308791540229761043805,$

so giebt (47.)

$$z = 5-2.38+4.4-8.61-97+2.22-4.40+8.15+79-2.8+4.3$$

oder

$$z = 5+16+44+120+79+12-(76+488+97+160+16) \text{ oder}$$
$$z = 276-837 = -561$$

und, wiederholt angewendet,

51. $z = 61-25 = 51.$

Hingegen (49.) giebt

$$z = -3+0-64+42+36-3+10-28-0+10-16+54+28-18$$
$$+2-0-4+15-64+0+20 \text{ oder}$$

52. $z = 217-200 = 17.$

Beide Z (51. u. 52.) gehen mit $s = 17$ auf; also geht auch Z (50.) mit 17 auf.

No. 8. Es sei

$$s = 19.$$

Hier kann man in (4.) $n=2$, $k=1$ setzen. Dieses giebt

53. $$2.10 = \mathfrak{G}19+1, \text{ also } r = 1,$$

folglich in (2.)

$$z = x_m + 2x_{m-1} + 2^2 x_{m-2} + 2^3 x_{m-3} + 2^4 x_{m-4} \ldots \text{ oder}$$

54. $$z = x_m + 2x_{m-1} + 4x_{m-2} + 8x_{m-3} - 3x_{m-4} - 6x_{m-5} + 7x_{m-6} - 5x_{m-6} + 9x_{m-7} - x_{m-7} - 2x_{m-1} - 4x_{m-2} \ldots$$

Es sei z. B.

55. $$Z = 13413966072992,$$

so giebt (54.)

$$z = 1+6+16+8-9-54+42-30+0-7-4-36-72+6 \text{ oder}$$
$$z = 79-212 = -133$$

und, wiederholt angewendet,

56. $$z = 1+6+12 = 19.$$

Dieses z geht mit 19 auf; also auch Z.

F. Es würde nützlich sein, nach dieser Art eine *Tafel*, wenigstens für alle Stammzahlen, etwa bis 1000, zu berechnen.

Für eine solche Tafel würde es immer am besten sein, in (4.) *n stets* $=1$ zu setzen. Ein anderer Werth von n kann zwar, wie sich an den obigen Beispielen zeigt, in einzelnen Fällen nützlich sein, aber wenn man eine voraus berechnete *Tafel* der Multiplicatoren der x in (2.) hat, nemlich eine Tafel der *echten Reste* der Multiplicatoren r^m, nr^{m-1}, n^2r^{m-2} etc. zu s, so ist es gleichgültig, was r in (4.) für $n=1$ ist: immer sind die Reste $<\frac{1}{2}s$. Außerdem aber hat man, wenn immer $n=1$ ist, noch den Vortheil, dafs, wenn Z *nicht* mit s aufgeht, z auch *denselben Rest* läfst wie Z, so dafs man also in solchem Falle *auch noch sogleich den Rest der Division von Z mit s findet;* was nicht unmittelbar geschieht, wenn n *nicht* gleich 1 ist. Für $n=1$ nemlich giebt (9. §. 32.) blofs

57. $$Z = \mathfrak{G}s + z,$$

und es folgt daraus, dafs, wenn man $Z = \mathfrak{G}s + \varrho_1$ und $z = \mathfrak{G}s + \varrho_2$ setzt, wo ϱ_1 und ϱ_2 beides die *unbedingt echten* Reste bezeichnen,

58. $$\mathfrak{G}s + \varrho_1 = \mathfrak{G}s + \mathfrak{G}s + \varrho_2 = \mathfrak{G}s + \varrho_2$$

sein mufs; was nicht anders sein kann, als wenn ϱ_1 *gleich* ϱ_2 ist, indem es *nur einen* unbedingt echten Rest zu s giebt.

Ferner wird es für die *Tafel* auch gut sein, in (4.) k *stets gleich* 1 zu setzen: denn in (2.), welches sich für $n=1$ auf

59. $z = x_m r^m + x_{m-1} r^{m-1} + x_{m-2} r^{m-2} + x_{m-3} r^{m-3} \dots + x_1 r + x_0,$

oder, wenn man die unbedingt echten Reste r^m, r^{m-1}, r^{m-2}, ... durch ϱ_m, ϱ_{m-1}, ϱ_{m-2}, ... bezeichnet, auf

60. $z = x_m \varrho_m + x_{m-1} \varrho_{m-1} + x_{m-2} \varrho_{m-2} \dots + x_1 \varrho_1 + x_0$

reducirt, sind die Multiplicatoren ϱ der x *immer* $<\frac{1}{2}s$. Ist nun $k=1$, so sind die x in (1.) oder (60.) die *einzelnen Ziffern* der Zahl Z, und z (60.) hat so viele Glieder als die Zahl Z einzelne Ziffern. Es kann also von dem ϱ *nur das 1* bis *9fache* zu nehmen vorkommen. Ist dagegen $k>1$, so hat zwar z in (60.) *weniger Glieder*, aber die x sind nun *mehrziffrige* Zahlen; eben wie die ϱ; letzteres wenn s einigermafsen grofs ist. Mehrziffrige Zahlen mit *einander* zu multipliciren, wird aber, selbst wenn es *weniger oft* vorkommt, doch immer schwieriger sein, als blofs die 1 bis 9fachen der mehrziffrigen Zahlen ϱ zu nehmen. Für *eine Tafel* ist das letztere aber noch *um so mehr* passend, da sich auch recht gut die 1 bis 9fachen der ϱ vorausberechnen lassen und sogleich in die Tafel aufgenommen werden können, nicht aber wohl die 1 bis 100 oder die 1 bis 1000fachen u. s. w. Enthält nun die Tafel auf diese Weise sogleich die 1 bis 9fachen der ϱ, im Voraus berechnet, so ist für z (60.) *gar keine Multiplication* weiter nöthig, sondern man kann die einzelnen Glieder der Reihe rechts in (60.) aus der Tafel unmittelbar *ablesen* und braucht nur die positiven wie die negativen Glieder zusammen- und die beiden Summen von einander abzuziehen.

G. Für die Tafel also würde man $n=1$ und $k=1$, folglich in (4.) blofs

61. $10 = \mathfrak{G}s + r$

zu setzen haben, welches, wenn $s>10$ ist, gradezu $r=10$ giebt. Also sind dann die ϱ in (60.) nichts andres als die *unbedingt echten* Reste der verschiedenen Potenzen von 10 selbst, zu s.

Für die Urzahl $s=857$ z. B. wäre

62. $$\begin{cases} 10 = \mathfrak{G}.857 + \varrho_1 & \text{und} \quad \varrho_1 = +\ 10, \\ 10^2 = \mathfrak{G}.857 + \varrho_2 & - \quad \varrho_2 = +\ 100, \\ 10^3 = \mathfrak{G}.857 + \varrho_3 & - \quad \varrho_3 = +\ 143, \\ 10^4 = \mathfrak{G}.857 + \varrho_4 & - \quad \varrho_4 = -284, \\ 10^5 = \mathfrak{G}.857 + \varrho_5 & - \quad \varrho_5 = -269, \\ \dots\dots & - \quad \dots\dots \end{cases}$$

Es würde daher, um zu finden, ob eine gegebene Zahl *Z* mit 857 aufgehe oder nicht, und welcher ***Rest*** im letzten Fall bleibe, von den Ziffern der Zahl *Z*, von der Rechten nach der Linken zu, die ***erste*** mit $+10$, die ***zweite*** mit $+100$, die ***dritte*** mit $+143$, die ***vierte*** mit -284, die ***fünfte*** mit -269 u. s. w. zu multipliciren sein, und die algebraische Summe dieser Producte würde z (60.) geben. Je nachdem dieses z mit 857 aufgeht, oder nicht, geht auch die gegebene Zahl *Z* mit 857 auf, oder nicht; und wenn z ***nicht*** mit 857 aufgeht, so ist der ***unbedingt echte*** Rest von z zu 857 ***derselbe***, wie der von *Z*.

Aber auch die 1 bis 9fachen der ϱ (62.), die vorkommen können, braucht man nicht so wie sie sind zu nehmen, sondern auch von ihnen nur die ***unbedingt echten Reste*** zu $s = 857$. So würde man z. B. für die Vielfachen von $\varrho_4 = -284$ nicht -284, -568, -852, -1136 u. s. w., sondern vielmehr nur -284, $+289$, $+5$, -279 u. s. w. zu nehmen haben. Findet man nun diese Vielfachen in der Tafel, so ist für z (60.) ***gar keine Multiplication*** weiter nöthig, sondern nur die ***Addition*** von Zahlen, die sich, ganz ausgerechnet, in der Tafel finden.

Die Tafel würde für die Stammzahl $s = 857$ Folgendes geben.

68.

Nummer der Ziffern von der Rechten zur Linken.	Werth der Ziffern.								
	1	2	3	4	5	6	7	8	9
1 . . .	+1	+2	+3	+4	+5	+6	+7	+8	+9
2 . . .	+10	+20	+30	+40	+50	+60	+70	+80	+90
3 . . .	+100	+200	+300	+400	−357	−257	−157	−57	+43
4 . . .	+143	+286	−428	−285	−142	+1	+144	+287	−427
5 . . .	−284	+289	+5	−279	+294	+10	−274	+299	+15
6 . . .	−269	+319	+50	−219	+369	+100	−169	+419	+150
7 . . .	−119	−238	−357	+381	+262	+143	+24	−95	−214
8 . . .	−333	+191	−142	+382	+49	−284	+240	−93	−426
9 . . .	+98	+196	+294	+392	−367	−269	−171	−73	+25
10 . . .	+123	+246	+369	−365	−242	−119	+4	+127	+250
11 . . .	+373	−111	+262	−222	+151	−333	+40	+413	−71
12 . . .	+302	−253	+49	+351	−204	+98	+400	−155	+147
13 . . .	−408	+41	−367	+82	−326	+123	−286	+164	−244
14 . . .	+205	+410	−242	−37	+168	+373	−279	−74	+131
15 . . .	+336	−185	+151	−370	−34	+302	−219	+117	−404
16 . . .	−68	−136	−204	−272	−340	−408	+381	+313	+245
17 . . .	+177	+354	−326	−119	+28	+205	+382	−298	−121
18 . . .	+56	+112	+168	+224	+280	+336	+392	−409	−353
19 . . .	−297	+263	−34	−331	+229	−68	−365	+195	−102
20 . . .	−399	+59	−340	+118	−281	+177	−222	+236	−163
21 . . .	+295	−267	+28	+323	−239	+56	+351	−211	+84
22 . . .	+379	−99	+280	−198	+161	−297	+82	−396	−17
23 . . .	+362	−133	+229	−266	+96	−399	−37	+325	−170
24 . . .	+192	+384	−281	−89	+103	+295	−370	−178	+14

Wenn nun z. B.

64. $Z = 8047398852147990496628954$

wäre, so hätte man wie folgt zu rechnen:

65.

Für die 1te Ziffer	4	...	+4		Für die 7te Ziffer	9	...	−214
- - 2te -	5	...	+50		- - 11te -	9	...	−71
- - 3te -	9	...	+43		- - 15te -	2	...	−185
- - 4te -	8	...	+287		- - 16te -	5	...	−340
- - 5te -	2	...	+289		- - 17te -	8	...	−298
- - 6te -	6	...	+100		- - 18te -	8	...	−409
- - 8te -	4	...	+382		- - 19te -	9	...	−102
- - 10te -	9	...	+250		- - 20te -	3	...	−340
- - 12te -	7	...	+400		- - 22te -	4	...	−198
- - 13te -	4	...	+82		- - 24te -	8	...	−178
- - 14te -	1	...	+205		Thut zusammen			−2335
- - 21te -	7	...	+351					+2443
Thut zusammen			+2443		Bleibt			+108

Die Zahl Z (64.) kann also mit $s = 857$ *nicht* aufgehen, sondern es mufs der Rest $+108$ bleiben; und so verhält es sich auch.

§. 34.

Lehrsatz.

Es seien u *und* v *zwei beliebige, zu einander theilerfremde positive ganze Zahlen.*

I. *Setzt man in der Gleichung*

1. $mv = nu + r$

der Reihe nach

2. $m = 0, 1, 2, 3, 4, \ldots . u-1$

und nimmt für alle r *die positiven oder die negativen echten Reste, deren zeichenfreie Werthe also alle* $< u$ *sind, so ist kein* r *dem andern gleich, und die zeichenfreien Werthe von* r *sind nothwendig alle die Zahlen*

3. $r = 0, 1, 2, 3, 4, \ldots . u-1,$

obwohl in anderer Aufeinanderfolge als die von m.

Zugleich sind alle $n < v$, *wenn* $v > u$ *ist. Ist* $v < u$, *so ist für diejenigen negativen* r, *welche mit* v *aufgehen und die sich dann unter den Werthen* (3.) *von* r *befinden,* $n = v$.

Zu dem Werth 0 *von* m *gehört* $r = 0$, *und zu* $r = 0$ *gehört* $m = 0$ *und* $n = 0$.

II. ***Für jedes beliebige positive oder negative*** r ***in*** (1.), ***auch*** $r=0$ ***nicht ausgenommen, so dafs also*** r ***allgemein durch***

$$4.\quad r = \varepsilon u + r_0$$

ausgedrückt werden kann, wo ε ***eine ganze positive oder negative Zahl und*** r_0 ***eine der Zahlen*** (3.) ***ist, giebt es immer unzählige zusammengehörige ganzzählige Werthe von*** m ***und*** n, ***welche der Gleichung*** (1.) ***genugthun. Sie werden allgemein durch***

$$5.\quad m = \lambda u + m_0 \quad \text{und}$$

$$6.\quad n = \lambda v + n_0 - \varepsilon$$

ausgedrückt, wo λ ***willkürlich ist, das zu*** r_0 ***in*** (1.) ***gehörige*** m_0 ***aber immer eine der Zahlen***

$$7.\quad m_0 = 0, 1, 2, 3, \ldots u-1$$

und das zu r_0 ***gehörige*** n_0 ***eine der Zahlen***

$$8.\quad n_0 = 0, 1, 2, 3, \ldots v-1$$

bezeichnet, mit Ausnahme von $r_0 = -v$ ***für*** $v<u$, ***wo*** $n_0 = v$ ***ist. Aufser den durch*** (5. u. 6.) ***ausgedrückten Werthen von*** m ***und*** n ***giebt es aber keine andern.***

III. ***Unter den unzähligen Werthen von*** m ***und*** n (5. u. 6.), ***die mit*** r (4.) ***der Gleichung*** (1.) ***genugthun, giebt es für jedes*** r ***immer einen und nur den einen positiven Werth*** $m_0<u$ ***von*** m ***und ein und nur das eine negative*** m_0-u, ***dessen zeichenfreier Werth*** $u-m_0$ ***ebenfalls*** $<u$ ***ist, aber nicht zugleich immer ein zugehöriges positives oder negatives*** n, ***dessen zeichenfreier Werth seinerseits*** $<v$ ***wäre, sondern letzteres nur in dem Falle, wenn in dem Ausdruck*** (4.) ***von*** r, $\varepsilon=0$, ***also der zeichenfreie Werth von*** r ***eine der Zahlen*** (3.) ***ist. In diesem einen Falle sind auch die zeichenfreien Werthe der zu*** m_0 ***und*** m_0-u ***gehörigen Werthe*** n_0 ***und*** n_0-v ***von*** n ***aus den Zahlen*** (8.), ***und wenn*** $v<u$ ***ist, so ist für*** r = ***den Vielfachen von*** $-v$, ***die*** $<u$ ***sind,*** $n_0=v$. ***Wir wollen die Werthe*** m_0 ***und*** m_0-u ***von*** m, ***nebst dem zugehörigen*** $n_0-\varepsilon$ ***und*** $n_0-\varepsilon-v$ ***von*** n ***kleinste Wurzeln der Gleichung*** (1.) ***nennen.***

IV. ***Wenn man dasjenige positive*** $m<u$ ***und das zugehörige positive*** $n<v$, ***welche in*** (1.) ***zu dem Rest*** $r=+1$ ***gehören, und welche nach*** (III.) ***immer Statt finden, durch*** m_1 ***und*** n_1 ***bezeichnet, so dafs also*** m_1 ***und*** n_1 ***zu dem Reste*** $+1$ ***die kleinsten positiven Wurzeln der Gleichung***

$$9.\quad mv = nu + 1$$

sind, so werden die kleinsten positiven und negativen Wurzeln der Gleichung (1.) *zu einem beliebigen Rest* r *durch*

$$10. \quad m_0 = m_1 r - \tau u \quad \textit{und} \quad m_1 r - (\tau + 1) u \quad \textit{und}$$

$$11. \quad n_0 - s = n_1 r - \tau v \quad \textit{und} \quad n_1 r - (\tau + 1) v$$

ausgedrückt, wo τu *in* (10.) *dasjenige Vielfache von* u *bedeutet, welches, von* $m_0 r$ *abgezogen, einen positiven Rest* $m_1 < u$ *läfst. In* (11.) *mufs* τ *denselben Werth bekommen, wie in* (10.), *wenn auch* $n_0 r - \tau v$ *nicht eine positive Zahl* $< v$ *ist.*

Beispiel. Es sei

$$12. \quad v = 15, \quad u = 22.$$

Setzt man hier der Reihe nach $m = 0, 1, 2, 3, \ldots 21$, so ergiebt sich

$$13. \left\{ \begin{array}{ll}
0.15 = 0.22 + 0 = 0.22 - 0 & 11.15 = 7.22 + 11 = 8.22 - 11 \\
1.15 = 0.22 + 15 = 1.22 - 7 & 12.15 = 8.22 + 4 = 9.22 - 18 \\
2.15 = 1.22 + 8 = 2.22 - 14 & 13.15 = 8.22 + 19 = 9.22 - 3 \\
3.15 = 2.22 + 1 = 3.22 - 21 & 14.15 = 9.22 + 12 = 10.22 - 10 \\
4.15 = 2.22 + 16 = 3.22 - 6 & 15.15 = 10.22 + 5 = 11.22 - 17 \\
5.15 = 3.22 + 9 = 4.22 - 13 & 16.15 = 10.22 + 20 = 11.22 - 2 \\
6.15 = 4.22 + 2 = 5.22 - 20 & 17.15 = 11.22 + 13 = 12.22 - 9 \\
7.15 = 4.22 + 17 = 5.22 - 5 & 18.15 = 12.22 + 6 = 13.22 - 16 \\
8.15 = 5.22 + 10 = 6.22 - 12 & 19.15 = 12.22 + 21 = 13.22 - 1 \\
9.15 = 6.22 + 3 = 7.22 - 19 & 20.15 = 13.22 + 14 = 14.22 - 8 \\
10.15 = 6.22 + 18 = 7.22 - 4 & 21.15 = 14.22 + 7 = 15.22 - 15
\end{array} \right.$$

Wäre dagegen

$$14. \quad v = 22, \quad u = 15,$$

so wäre

$$15. \left\{ \begin{array}{ll}
0.22 = 0.15 + 0 = 0.15 - 0 & 8.22 = 11.15 + 11 = 12.15 - 4 \\
1.22 = 1.15 + 7 = 2.15 - 8 & 9.22 = 13.15 + 3 = 14.15 - 12 \\
2.22 = 2.15 + 14 = 3.15 - 1 & 10.22 = 14.15 + 10 = 15.15 - 5 \\
3.22 = 4.15 + 6 = 5.15 - 9 & 11.22 = 16.15 + 2 = 17.15 - 13 \\
4.22 = 5.15 + 13 = 6.15 - 2 & 12.22 = 17.15 + 9 = 18.15 - 6 \\
5.22 = 7.15 + 5 = 8.15 - 10 & 13.22 = 19.15 + 1 = 20.15 - 14 \\
6.22 = 8.15 + 12 = 9.15 - 3 & 14.22 = 20.15 + 8 = 21.15 - 7 \\
7.22 = 10.15 + 4 = 11.15 - 11 &
\end{array} \right.$$

a. Wie (13. u. 15.) zeigen, sind die positiven so wie die negativen Reste alle unter einander *verschieden*, und beide sind in (13.) die Zahlen 0, 1, 2, 3, ... 21 ($= u - 1$) und in (15.) die Zahlen 0, 1, 2, 3, ... 14

$(=u-1)$. Desgleichen sind in (15.), wo $v > u$ ist, alle n ohne Ausnahme $< v (= 22)$. In (13.) dagegen, wo $v < u$, ist *für den* Rest $r = -u = -15$, $n = 15 = v$. Die übrigen n sind ebenfalls alle $< v$. Desgleichen gehört überall zu $m = 0$, $r = 0$, und zu $r = 0$ gehört $m = 0$ und $n = 0$. Dieses zusammen ist was (I.) behauptet.

b. Es sei für (12.)

16. $r = 141 = 6.u + 9$, also in (4.) $\varepsilon = 6$, $r_0 = 9$.

Die zu $r_0 = 9$ gehörigen m_0 und n_0 sind zufolge (13.) $= 5$ und 3: also ist nach (5. u. 6.)

17. $\begin{cases} m = \pm(1, 2, 3, \ldots .)22 + 5 \quad \text{und} \\ n = \pm(1, 2, 3, \ldots .)15 + 3 - 6 = (1, 2, 3, \ldots .)15 - 3. \end{cases}$

Man setze z. B. das *willkürliche* λ in (4. u. 5.) $= 4$, so ist nach (17.)

18. $\begin{cases} m = 4.22 + 5 = 93 \quad \text{und} \\ n = 4.15 - 3 = 57. \end{cases}$

Diese m und n müssen also der Gleichung (1.) zu $r = 141$ genugthun, das heifst, es mufs

19. $93.15 = 57.22 + 141$

sein; was auch der Fall ist.

Die *kleinsten* von den Werthen von m und n (17.) sind diejenigen für $\lambda = 0$, also $m = 5 < u$ und $n = -3$, welches die Werthe $m_0 = 5$ und $n_0 - \varepsilon = 3 - 6 = -3$ *selbst* sind; desgleichen sind es diejenigen für $\lambda = -1$, also $m = -17$ und $n = -18$, wo der zeichenfreie Werth 17 von m ebenfalls $< u$ ist. Also müssen auch die Werthe 5 und -17 von m, und -3 und -18 von n der Gleichung (1.) zu dem Rest $r = 141$ genugthun, das heifst, es mufs

20. $\begin{cases} +\ 5.15 = -\ 3.22 + 141 \quad \text{und} \\ -17.15 = -18.22 + 141 \end{cases}$

sein; was auch der Fall ist.

c. Es sei für (14.)

21. $r = -55 = -4.u + 5$, so dafs in (4.) $\varepsilon = -4$, $r_0 = 5$.

Die zu $r_0 = 5$ gehörigen m_0 und n_0 sind zufolge (15.) $= 5$ und 7, also ist nach (5. u. 6.)

22. $\begin{cases} m = \pm(1, 2, 3, \ldots .)15 + 5 \quad \text{und} \\ n = \pm(1, 2, 3, \ldots .)22 + 7 + 4. \end{cases}$

Man setze das *willkurliche* λ in (4. u. 5.) $= -2$, so ist nach (22.)

$$23. \quad \begin{cases} m = -2.15+5 = -25 \quad \text{und} \\ n = -2.22+11 = -33 \end{cases}$$

Diese m und n müssen der Gleichung (1.) zu $r=-55$ genugthun, das heifst, es mufs

$$24. \quad -25.22 = -33.15-55$$

sein; was auch der Fall ist.

Die *kleinsten* von den Werthen von m und n (22.) sind wieder diejenigen für $\lambda=0$, also $m=5<u$ und $n=11$, welches die Werthe von $m_{\prime\prime}=5$ und $n_{\prime\prime}-s=7-(-4)=11$ *selbst* sind; desgleichen sind es diejenigen für $\lambda=-1$, also $m=-10$ und $n=-11$, wo der zeichenfreie Werth 10 von m ebenfalls $<u$ ist. Also müssen auch die Werthe 5 und -10 von m und 11 und -11 von n der Gleichung (1.) zu dem Reste $r=-55$ genugthun, das heifst es mufs

$$25. \quad \begin{cases} +5.22 = +11.15-55 \quad \text{und} \\ -10.22 = -11.15-55 \end{cases}$$

sein; was auch der Fall ist.

Die Resultate in (*b.* u. *c.*) sind den Behauptungen in (II. u. III.) gemäfs.

d. Für (12.) ist zufolge (13.) dasjenige m und n, welches dem Rest $+1$ entspricht, $=3$ und 2, so dafs also für (12.)

$$26. \quad m_1 = 3 \quad \text{und} \quad n_1 = 2$$

ist. Nun sei, wie in (16.),

$$27. \quad r = 141,$$

so giebt (10. u. 11.)

$$28. \quad \begin{cases} m_{\prime\prime}=3.141-19.22=+5, \text{ also } \tau=19 \text{ und } m_{\prime\prime}=3.141-20.22=-17 \text{ und} \\ n_{\prime\prime}=2.141-19.15=-3 \text{ und } \qquad n_{\prime\prime}=2.141-20.15=-18, \end{cases}$$

und diese $m_{\prime\prime}$ und $n_{\prime\prime}$ müssen der Gleichung (1.) für den Rest $r=141$ genugthun; was auch zufolge (20.) der Fall ist.

e. Für (14.) ist zufolge (15.) dasjenige m und n, welches dem Rest $+1$ entspricht $=13$ und 19, so dafs also für (14.)

$$29. \quad m_1 = 13 \quad \text{und} \quad n_1 = 19$$

ist. Nun sei, wie in (21.),

$$30. \quad v = -55,$$

so giebt (10. und 11.)

$$31. \quad \begin{cases} m_{\prime\prime}=-13.55+48.15=+5, \text{ also } \tau=-48 \text{ und } m_{\prime\prime}=-13.55+47.15=-10 \text{ und} \\ n_{\prime\prime}=-19.55+48.22=+11 \text{ und } \qquad n_{\prime\prime}=-19.55+47.22=-11, \end{cases}$$

und diese $m_{\prime\prime}$ und $n_{\prime\prime}$ müssen der Gleichung (1.) für den Rest $r=-55$ genugthun; was auch zufolge (25.) der Fall ist.

Die Resultate (*d.* u. *e.*) sind den Behauptungen in (IV.) gemäfs.

Beweis. *A.* Gäben zwei verschiedene m, z. B. m_β und m_γ, beide $<u$, mit den dazu gehörigen n_β und n_γ *ein und dasselbe* r, so dafs also

$$32.\quad \begin{cases} m_\beta v = n_\beta u \pm r \text{ und} \\ m_\gamma v = n_\gamma u \pm r \end{cases}$$

wäre, so würde daraus

$$33.\quad (m_\beta - m_\gamma)v = (n_\beta - n_\gamma)u$$

folgen, und also müfste $m_\beta - m_\gamma$ mit u *aufgehen*, da v nach der Voraussetzung keinen Theiler mit u gemein hat (§. 25.) Dieses kann aber nicht sein, da m_β und m_γ beide $<u$ sind und folglich auch $m_\beta - m_\gamma < u$ ist. Also können keine zwei m, beide $<u$, *einen und denselben* Rest $\pm r$ lassen, und folglich sind *alle* zu $m = 1, 2, 3, \ldots u-1$ gehörigen r *von einander verschieden.*

Die *Anzahl* der r ist aber der der Werthe von m *gleich*, und folglich $= u$. Zugleich sollen die zeichenfreien Werthe aller $r<u$ sein. Also sind diese zeichenfreien Werthe der r nothwendig *alle* die u Zahlen 0, 1, 2, 3, ... $u-1$ selbst; gemäfs (3.)

B. Der *gröfste* Werth von n findet in (1.) offenbar für den *gröfsten* Werth von m Statt, also für $m = u-1$. Man setze für $m = u-1$ in (1.)

$$34.\quad (u-1)v = xu + r.$$

Soll hier r *positiv* sein, so kann x nicht $= v$ sein, selbst nicht für $r=0$; denn $x = v$ würde immer $xu = vu > (u-1)v$ geben. Folglich ist für *positive* r, x, also n, *immer* $<v$.

Soll r *negativ* sein, so folgt aus

$$35.\quad (u-1)v = v.u - v = (v+x)u - (xu+v),$$

dafs nur dann

$$36.\quad n = v + x$$

sein kann, wenn

$$37.\quad xu + v < u$$

ist; denn der absolute Werth $xu+v$ des Restes in (35.) soll *immer* $<u$ sein. Die Bedingung (37.) ist aber nur für $x=0$ erfüllbar; denn für *jedes* gröfsere x ist $xu+v$ nicht $<u$, sondern $>u$, was auch v sein mag. *Nie* also kann zufolge (36.) $n>v$ sein. Es kann höchstens $=v$ sein, und dieses zufolge (37.) nur dann wenn $v<u$ ist. Nun ist für ein *beliebiges* $u-\mu$fache von v:

$$38.\quad (u-\mu)v = v.u - \mu v.$$

Ist nun $v<u$, so kann auch noch $\mu v < u$ sein. Also für alle die Reste $-v$, $-2v$, $-3v$, ... $-\mu v$, die auch *alle* vorkommen, ist $n = v$.

Zusammen also folgt, dafs n für $v>u$ *immer* $<v$ ist; desgleichen auch für $v<u$, ausgenommen wenn der *negative Rest* mit v *aufgeht*; wie solches der Lehrsatz in (1.) behauptet.

C. Ist $m=0$, so giebt (1.)

$$39. \quad 0 = nu+r.$$

Also mufs r mit u *aufgehen* (§. 18.). Dieses geschieht nur dann, wenn $r=0$ ist, indem r jedenfalls $<u$ sein soll. Also ist für $m=0$, $r=0$, und folglich vermöge (39.) auch $n=0$.

Ist $r=0$, so giebt (1.)

$$40. \quad mv = nu,$$

also mufs m mit u *aufgehen* (§. 25.). Dieses ist nur möglich, wenn $m=0$ ist, indem $m<u$ sein soll. Also ist für $r=0$, $m=0$, und folglich vermöge (40.) auch $n=0$.

So behauptet es (I.).

D. Setzt man (5., 6. und 4.) in (1.), so ergiebt sich

$$(\lambda u+m_0)v = (\lambda v+n_0-\varepsilon)u+\varepsilon u+r_0 \quad \text{oder}$$

$$41. \quad m_0 v = n_0 u+r_0.$$

Diese Gleichung entspricht der (1.) mit allen den Werthen (7.) von m_0, (8.) von n_0 und (3.) von r_0. Also thun alle die durch (5. u. 6.) ausgedrückten Werthe von m und n mit jedem *beliebigen* λ der Gleichung (1.) ein Genüge; wie es (II.) behauptet.

E. Gäbe es noch andere Werthe von m und n, als die, welche (5. u. 6.) ausdrückt, so könnten es nur solche sein, die durch

$$42. \quad m = \lambda u+m_0+\mu \quad \text{und}$$

$$43. \quad n = \lambda v+n_0-\varepsilon+\nu$$

ausgedrückt werden, wo μ eine Zahl ist, die *nicht* mit u, ν eine Zahl, die *nicht* mit v *aufgeht;* denn ginge μ mit u auf, so wäre (42.) schon in (5.) und (43.) schon in (6.) *mitbegriffen,* indem dort λ *willkürlich* ist. Setzt man nun (42. u. 43.) nebst (4.) in (1.), so ergiebt sich

$$(\lambda u+m_0+\mu)v = (\lambda v+n_0-\varepsilon+\nu)u+\varepsilon u+r_0 \quad \text{oder}$$

$$44. \quad m_0 v+\mu v = n_0 u+\nu u+r_0.$$

Hiervon die Gleichung (41.), die nothwendig zugleich Statt findet, abgezogen, giebt

$$45. \quad \mu v = \nu u.$$

Dieses ist wieder nur möglich, wenn μ mit u und ν mit v *aufgeht* (§. 25.). Und da dies *nicht* sein *soll,* so finden die Ausdrücke (42. u. 43.) von m und

n nicht Statt: mithin giebt es aufser den Werthen von m und n, welche (5. u. 6.) ausdrückt, *keine andern*; wie es (II.) behauptet.

F. Da λ in (5. u. 6.) willkürlich ist, so kann es auch 0 und -1 sein. Dieses giebt

$$46. \quad m = m_0 \quad \text{und} \quad m = m_0 - u \quad \text{und}$$

$$47. \quad n = n_0 - \varepsilon \quad \text{und} \quad n = n_0 - \varepsilon - v.$$

Hier sind m_0 und $m_0 - u$ dieselben beiden m, (an zeichenfreien Werth beide $< u$) welche der Gleichung (1.) für Reste $< u$ genugthun. Also thun *dieselben beiden* m auch der Gleichung (1.) für *beliebige* Reste r (4.) genug. Dagegen sind die *zugehörigen* beiden Werthe $n_0 - \varepsilon$ und $n_0 - \varepsilon - v$ von n *nicht* nothwendig $< v$. Sie sind es nur, wenn $\varepsilon = 0$, also r eine der Zahlen (3.) ist.

Dieses ist, was (III.) behauptet.

G. Multiplicirt man die in (IV.) vorausgesetzte Gleichung

$$48. \quad m_1 v = n_1 u + 1$$

mit r, so ergiebt sich

$$49. \quad m_1 r v = n_1 r u + r.$$

Hiervon die Gleichung

$$50. \quad m_0 v = (n_0 - \varepsilon) u + r,$$

die sich ergiebt, wenn man (5. u. 6.) in (1.) und das willkürliche $\lambda = 0$ setzt, abgezogen, giebt

$$51. \quad (m_1 r - m_0) v = (n_1 r - (n_0 - \varepsilon)) u.$$

Dieser Gleichung gemäfs mufs $m_1 r - m_0$ mit u aufgehen (§. 25.) und also

$$52. \quad m_1 r - m_0 = \tau u$$

sein, wo τ irgend eine *ganze* Zahl ist. Ferner giebt (52.), in (51.) gesetzt,

$$\tau u v = (n_1 r - (n_0 - \varepsilon)) u, \text{ also}$$

$$53. \quad \tau v = n_1 r - (n_0 - \varepsilon).$$

Aus (52. u. 53.) folgt (10. u. 11.) zunächst für ein *positives* $m_0 < u$, und dann, wenn man noch u und v abzieht, also $\tau + 1$ statt τ schreibt, auch für ein negatives m_0, dessen absoluter Werth $< u$ ist.

Dies ist, was (IV.) behauptet.

H. Anm. Ein Hauptpunct des Beweises ist das Mittel, durch welches in (*A.*) gezeigt wird, dafs nicht zwei verschiedene Vielfachen von v zu u *gleiche* Reste lassen können. Es kommt sehr häufig zur Anwendung. Dann der Schlufs, dafs die Reste, weil sie alle verschieden und $> v$ und $< u$ sind, die Zahlen 1, 2, 3, 4, ... $u - 1$ selbst sein müssen. Auch dieser Schlufs kommt öfter vor.

§. 35.

Lehrsatz.

Es seien u *und* v *zwei beliebige zu einander* ***theilerfremde positive ganze Zahlen.***

Setzt man in der Gleichung

$$1.\quad \mathrm{mv} = \mathfrak{G}\mathrm{u} + \mathrm{r}$$

der Reihe nach

$$2.\quad \mathrm{m} = 1, 2, 3, 4, \ldots \tfrac{1}{2}(\mathrm{u}-1), \quad \textit{wenn } \mathrm{u} \textit{ ungerade, und}$$

$$3.\quad \mathrm{m} = 1, 2, 3, 4, \ldots \tfrac{1}{2}\mathrm{u}, \quad \textit{wenn } \mathrm{u} \textit{ gerade ist,}$$

und bezeichnet diejenigen Werthe von m, *welche in* (1.) ***positive Reste*** $\mathrm{r} > \frac{1}{2}\mathrm{u}$ ***geben,*** *durch* $\mathrm{m}_1, \mathrm{m}_2, \mathrm{m}_3, \ldots \mathrm{m}_x$, *die übrigen Werthe von* m, *welche positive Reste* ***nicht*** $>\frac{1}{2}\mathrm{u}$ ***geben,*** *durch* $\mu_1, \mu_2, \mu_3, \ldots \mu_{\frac{1}{2}(\mathrm{u}-1)-x}$ *oder* $\mu_{\frac{1}{2}\mathrm{u}-x}$, *setzt darauf für alle* r, *die* $>\frac{1}{2}\mathrm{u}$ *sind,*

$$4.\quad \mathrm{r} = \mathrm{u} - \varrho,$$

wo nun also auch alle ϱ, *eben wie die übrigen* r, ***nicht grösser als*** $\frac{1}{2}\mathrm{u}$ *sind, so dass zusammengenommen*

***Erstlich für ein* ungerades u:**

$$5.\ \begin{cases} \mathrm{m}_1\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_1, \\ \mathrm{m}_2\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_2, \\ \mathrm{m}_3\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_3, \\ \ldots\ldots\ldots\ldots \\ \mathrm{m}_{\frac{1}{2}(\mathrm{u}-1)-x}\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_{\frac{1}{2}(\mathrm{u}-1)-x} \end{cases} \quad \text{und} \quad 6.\ \begin{cases} \mu_1\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_1, \\ \mu_2\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_2, \\ \mu_3\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \mu_x\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_x; \end{cases}$$

***Zweitens für ein* gerades u:**

$$7.\ \begin{cases} \mathrm{m}_1\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_1, \\ \mathrm{m}_2\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_2, \\ \mathrm{m}_3\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_3, \\ \ldots\ldots\ldots\ldots \\ \mathrm{m}_{\frac{1}{2}\mathrm{u}-x}\mathrm{v} = \mathfrak{G}\mathrm{u} + \mathrm{r}_{\frac{1}{2}\mathrm{u}-x} \end{cases} \quad \text{und} \quad 8.\ \begin{cases} \mu_1\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_1, \\ \mu_2\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_2, \\ \mu_3\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \mu_x\mathrm{v} = \mathfrak{G}\mathrm{u} - \varrho_x \end{cases}$$

ist, so sind die absoluten Werthe der r *und* ϱ ***zusammengenommen*** *nothwendig*

9. *Im ersten Falle* (5. u. 6.) *alle die Zahlen* $1, 2, 3, 4, \ldots \frac{1}{2}(\mathrm{u}-1)$ und
10. *Im zweiten Falle* (7. u. 8.) *alle die Zahlen* $1, 2, 3, 4, \ldots \frac{1}{2}\mathrm{u}$.

Beispiele. 1. Es sei

$$11.\quad u = 15, \quad v = 22.$$



so ist

12. $(1, 2, 3, 4, 5, 6, 7)v = \mathfrak{G}u + 7, 14, 6, 13, 5, 12$ und 4.

Von diesen Resten sind die $x = 3$ Reste, 14, 13 und $12 > \frac{1}{2}u$, also ist in (5. u. 6.)

13. $(1, 2, 3, 4, 5, 6, 7)v = \mathfrak{G}u + 7, -1, +6, -2, +5, -3$ und $+4$.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7; gemäfs (9.).

2. Es sei

$$14. \quad u = 15, \quad v = 4,$$

so ist

15. $(1, 2, 3, 4, 5, 6, 7)v = Nu + 4, 8, 12, 1, 5, 9$ und 13.

Von diesen Resten sind die $x = 4$ Reste 8, 12, 9 und $13 > \frac{1}{2}u$, also ist in (5. und 6.)

16. $(1, 2, 3, 4, 5, 6, 7)v = \mathfrak{G}u + 4, -7, -3, +1, +5, -6$ und -2.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7; gemäfs (9.).

3. Es sei

$$17. \quad u = 18, \quad v = 49,$$

so ist

18. $(1, 2, 3, 4, 5, 6, 7, 8, 9)v = \mathfrak{G}u + 13, 8, 3, 16, 11, 6, 1, 14$ und 9.

Von diesen Resten sind die $x = 4$ Reste 13, 16, 11 und $14 > \frac{1}{2}u$, also ist in (7. u. 8.)

19. $(1, 2, 3, 4, 5, 6, 7, 8, 9)v = \mathfrak{G}u - 5, +8, +3, -2, -7, +6, +1, -4$ und $+9$.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 3, 4, 5, 6, 7, 8, 9; gemäfs (10.).

4. Es sei

$$20 \quad u = 22, \quad v = 15,$$

so ist

21. $(1, 2, 3, \ldots 11)v = \mathfrak{G}u + 15, 8, 1, 16, 9, 2, 17, 10, 3, 18, 11$.

Von diesen Resten sind die $x = 4$ Reste 15, 16, 17 und $18 > \frac{1}{2}u$, also ist in (7. u. 8.)

22. $(1, 2, 3, \ldots 11)v = \mathfrak{G}u - 7, +8, +1, -6, +9, +2, -5, +10, +3, -4, +11$.

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 und 11; gemäfs (10.).

Beweis. *A.* Kein r in (1.) kann $=0$ sein. Denn für $r=0$ wäre in (1.) $mv=\mathfrak{G}u$, also müfste m mit u aufgehen, da v zu u *theilerfremd* sein soll (§. 25.). m geht aber nicht mit u auf, weil alle $m<u$ sind (2. u. 3.); also kann r nicht $=0$ sein.

B. Wäre in (5. oder 7.) irgend ein r einem andern gleich, also z. B.

$$23.\quad m_\epsilon v=\mathfrak{G}u+r \quad \text{und} \quad m_\lambda v=\mathfrak{G}u+r,$$

so würde daraus

$$24.\quad (m_\epsilon-m_\lambda)v=\mathfrak{G}u$$

folgen, und also müfste $m_\epsilon-m_\lambda$ mit u aufgehen (§. 25.). Dieses ist aber nicht der Fall, da m_ϵ und m_λ beide $<u$ sind und also $m_\epsilon-m_\lambda$ noch um so mehr $<u$ ist. Daher kann *kein r dem andern gleich sein.*

C. Ganz aus *gleichen* Gründen kann in (6. oder 8.) kein ϱ dem andern gleich sein.

D. Wäre in (5. und 6.) oder in (7. und 8.) ein r einem ϱ gleich, also z. B.:

$$25.\quad m_\epsilon v=\mathfrak{G}u+r \quad \text{und} \quad \mu_\lambda v=\mathfrak{G}u+r$$

so würde daraus

$$26.\quad (m_\epsilon+\mu_\lambda)v=\mathfrak{G}u$$

folgen; also müfste $m_\epsilon+\mu_\lambda$ mit u aufgehen (§. 25.). Aber in (5. und 6.) sind *alle* m oder $\mu<\frac{1}{2}u$ (2.) und in (7. und 8.) kann *nur eines* der m oder $\mu=\frac{1}{2}u$ sein (3.), die andern sind nothwendig *kleiner: folglich* ist *immer* $m_\epsilon+\mu_\lambda<u$. Mithin kann $m_\epsilon+\mu_\lambda$ *nicht* mit u aufgehen, und folglich kann in (5. und 6.), eben wie (7. und 8.), *kein r einem ϱ gleich sein.* Die r und ϱ sind also *alle* unter einander verschieden, und keins ist 0.

E. Nun ist die *Anzahl* der r und ϱ zusammengenommen der der m *gleich,* also in (5. und 6.) $=\frac{1}{2}(u-1)$ (2.) und in (7. und 8.) $=\frac{1}{2}u$ (3.) keins ist gröfser als $\frac{1}{2}u$, und alle sind von einander verschieden (*B.*, *C.* und *D.*). Also sind die r und ϱ zusammengenommen in (5. und 6.) nothwendig die Zahlen $1, 2, 3, \ldots \frac{1}{2}(u-1)$, und in (7. und 8.) nothwendig die Zahlen $1, 2, 3, \ldots \frac{1}{2}u$ selbst; wie es der Lehrsatz in (9. und 10.) behauptet.

F. Anm. Die in der Anmerkung zum vorigen Parapraph erwähnten Schlüsse sind auch hier die Hauptmomente des Beweises.

§. 36.

Lehrsatz.

Es seien u *und* v *zwei beliebige ungerade und zu einander theilerfremde ganze Zahlen und* z *sei eine beliebige positive ganze Zahl*

$$1.\quad z<\tfrac{1}{2}uv.$$

Alsdann können, wenn man für ein und dasselbe z,

$$2.\quad z = m_1u + r \quad \textit{und}$$
$$3.\quad z = m_2v + \varrho$$

setzt, wo r *und* ϱ *die echten positiven Reste zu* u *und* v *bezeichnen, so daß immer*

$$4.\quad r < u \quad \textit{und} \quad \varrho < v$$

ist, folgende verschiedene Fälle stattfinden.

5\. *Erstlich, wenn* $r > \frac{1}{2}u$ *ist, kann*
1) $\varrho = 0$,
2) $\varrho < \frac{1}{2}v > 0$,
3) $\varrho > \frac{1}{2}v$ *sein.*

Zweitens, wenn $r < \frac{1}{2}u > 0$ *ist, kann*
1) $\varrho = 0$,
2) $\varrho < \frac{1}{2}v > 0$ *und*
3) $\varrho > \frac{1}{2}v$ *sein.*

Drittens, wenn $r = 0$ *ist, kann*
1) $\varrho < \frac{1}{2}v > 0$ *und*
2) $\varrho > \frac{1}{2}v$ *sein.*

Bezeichnet man für diese 8 Fälle die Anzahl der $z < \frac{1}{2}uv$,

6\.

1)	*für welche*	$r > \frac{1}{2}u$	*und*	$\varrho = 0$	*ist, durch*	n_1,
2)	- - -	$r > \frac{1}{2}u$	-	$\varrho < \frac{1}{2}v > 0$	- - -	n_2,
3)	- - -	$r > \frac{1}{2}u$	-	$\varrho > \frac{1}{2}v$	- - -	n_3,
4)	- - -	$r < \frac{1}{2}u > 0$	-	$\varrho = 0$	- - -	n_4,
5)	- - -	$r < \frac{1}{2}u > 0$	-	$\varrho < \frac{1}{2}v > 0$	- - -	n_5,
6)	- - -	$r < \frac{1}{2}u > 0$	-	$\varrho > \frac{1}{2}v$	- - -	n_6,
7)	- - -	$r = 0$	-	$\varrho < \frac{1}{2}v > 0$	- - -	n_7,
8)	- - -	$r = 0$	-	$\varrho > \frac{1}{2}v$	- - -	n_8,

so ist

Erstlich, die Gesammtheit aller dieser verschiedenen z,

$$7\quad n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \tfrac{1}{2}(uv - 1).$$

Zweitens, die Anzahl der $n_7 + n_8$ *mit* u *aufgehenden* z *ist*

$$8.\quad n_7 + n_8 = \tfrac{1}{2}(v - 1).$$

Drittens, die Anzahl der $n_1 + n_4$ *mit* v *aufgehenden* z *ist*

$$9.\quad n_1 + n_4 = \tfrac{1}{2}(u - 1)$$

Viertens, die Anzahl der $n_2+n_5+n_7$ *verschiedenen* z, *welche, mit* v *dividirt, Reste* $\rho<\frac{1}{2}v>0$ *lassen, gleichviel welche Reste* r *sie mit* u *dividirt geben mögen, ist*

$$10. \quad n_2+n_5+n_7 = \tfrac{1}{4}(u+1)(v-1).$$

Fünftens, die Anzahl der $n_4+n_5+n_6$ *verschiedenen* z, *welche, mit* u *dividirt, Reste* $r<\frac{1}{2}u>0$ *lassen, gleichviel welche Reste* ρ *sie mit* v *dividirt geben mögen, ist*

$$11. \quad n_4+n_5+n_6 = \tfrac{1}{4}(u-1)(v+1).$$

Sechstens, die Anzahl der $n_3+n_6+n_8$ *verschiedenen* z, *welche, mit* v *dividirt, Reste* $\rho>\frac{1}{2}v$ *lassen, gleichviel welche Reste* r *sie mit* u *dividirt geben mögen, ist*

$$12. \quad n_3+n_6+n_8 = \tfrac{1}{4}(u-1)(v-1).$$

Siebentens, die Anzahl der $n_1+n_2+n_3$ *verschiedenen* z, *welche mit* u *dividirt Reste* $r>\frac{1}{2}u$ *lassen, gleichviel welche Reste* ρ *sie mit* v *dividirt geben mögen, ist*

$$13. \quad n_1+n_2+n_3 = \tfrac{1}{4}(u-1)(v-1).$$

Achtens, die Anzahl der n_3+n_5 *verschiedenen* z, *welche mit* u *und mit* v *dividirt entweder* ***zugleich*** *Reste* $r>\frac{1}{2}u$ *und* $\rho>\frac{1}{2}v$, *oder* ***zugleich*** *Reste* $r<\frac{1}{2}u>0$ *und* $\rho<\frac{1}{2}v>0$ *lassen, ist*

$$14. \quad n_3+n_5 = \tfrac{1}{4}(u-1)(v-1).$$

Neuntens, die Anzahl der n_2+n_6 *verschiedenen* z, *welche mit* u *und mit* v *dividirt entweder* ***zugleich*** *Reste* $r>\frac{1}{2}u$ *und* $\rho<\frac{1}{2}v>0$, *oder* ***zugleich*** *Reste* $r<\frac{1}{2}u>0$ *und* $\rho>\frac{1}{2}v$ *lassen, ist*

$$15. \quad n_2+n_6 = \tfrac{1}{4}(u-1)(v-1).$$

Zehntens, die doppelte Anzahl $2n_5$ *derjenigen* z, *welche mit* u *und mit* v *dividirt* ***zugleich*** *Reste* $r<\frac{1}{2}u>0$ *und* $\rho<\frac{1}{2}v>0$ *lassen, weniger der Anzahl* n_1 *derjenigen mit* v ***aufgehenden*** z, *welche mit* u *dividirt Reste* $>\frac{1}{2}u$ *lassen, und der mit* u ***aufgehenden*** n_8 *Zahlen* z, *welche mit* v *dividirt Reste* $>\frac{1}{2}v$ *lassen, ist*

$$16. \quad 2n_5-n_1-n_8 = \tfrac{1}{4}(u-1)(v-1).$$

Elftens, die Anzahl der mit v ***aufgehenden*** n_1 *verschiedenen* z, *welche Reste* $>\frac{1}{2}u$ *lassen, zusammen mit der Anzahl der* n_8 *mit* u ***aufgehenden*** z, *welche Reste* $>\frac{1}{2}v$ *lassen, und der Anzahl* n_3 *der* z, *welche mit* u *und* v *dividirt* ***zugleich*** *Reste* $r>\frac{1}{2}u$ *und* $\rho>\frac{1}{2}v$ *lassen, ist der Anzahl* n_4 *derjenigen* z ***gleich***, *welche mit* u *und* v *dividirt zugleich Reste* $r<\frac{1}{2}u>0$ *und* $\rho<\frac{1}{2}v>0$ *lassen,*

das heifst, es ist

$$17.\quad n_1+n_6+n_3=n_5.$$

Beispiel. Es sei

$$18.\quad u=7,\quad v=11,\quad \text{also}\quad uv=77\quad\text{und}$$

$$19.\quad z=1,\ 2,\ 3,\ 4,\ \ldots.\ 38\left(=\tfrac{1}{2}(uv-1)\right),$$

so geben die beiden Gleichungen (2. u. 3.) Folgendes:

20.

Für $z=$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
ist $m_1=$	0	0	0	0	0	0	1	1	1	1	1	1	1	2	2	2	2	2	2
$r=$	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5
$m_2=$	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
$\varrho=$	1	2	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
21.	5	5	5	2	2	3	8	6	6	6	1	2	2	7	5	5	6	3	3

Für $z=$	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
ist $m_1=$	2	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5	5	5
$r=$	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3
$m_2=$	1	1	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3
$\varrho=$	9	10	0	1	2	3	4	5	6	7	8	9	10	0	1	2	3	4	5
21.	3	8	4	5	5	2	2	2	8	6	6	6	3	1	2	7	5	5	5

Die horizontale Zeile (21.) giebt die *Nummer* der 8 Classen (6.) an, in welche jedes z gehört. Z. B.: Für $z=17$ ist $r=3<\frac{1}{2}u>0$ und $\varrho=6>\frac{1}{2}v$, also gehört $z=17$ in die *sechste* Classe (6.); und so die andern. Zufolge (21.) gehören also

22.
- die 2 Zahlen 11 und 33 in die *erste* Classe, folglich ist hier $n_1=2$;
- die 8 Zahlen 4, 5, 12, 13, 25, 26, 27 und 34 gehören in die *zweite* Classe, also ist $n_2=8$;
- die 5 Zahlen 6, 18, 19, 20 und 32 gehören in die *dritte* Classe, also ist $n_3=5$;
- die 1 Zahl 22 gehört in die *vierte* Classe, also ist . . $n_4=1$;
- die 10 Zahlen 1, 2, 3, 15, 16, 23, 24, 36, 37 und 38 gehören in die *fünfte* Classe, also ist $n_5=10$;
- die 7 Zahlen 8, 9, 10, 17, 29, 30, 31 gehören in die *sechste* Classe, also ist $n_6=7$;
- die 2 Zahlen 14 und 35 gehören in die *siebente* Classe, also ist $n_7=2$;
- die 3 Zahlen 7, 21 und 28 gehören in die *achte* Classe, also ist $n_8=3$.

Diese Werthe der verschiedenen n thun nun wie folgt den Gleichungen (7. bis 17.) des Lehrsatzes Genüge. Nemlich

23.
- die Gleichung (7.) ist hier $2+8+5+1+10+7+2+3=38=\frac{1}{2}(uv-1)$,
- \- \- \- (8.) \- \- $2+3=5=\frac{1}{2}(v-1)$,
- \- \- \- (9.) \- \- $2+1=3=\frac{1}{2}(u-1)$,
- \- \- \- (10.) \- \- $8+10+2=20=\frac{1}{4}(u+1)(v-1)=\frac{1}{4}.8.10$,

$$23.\quad\begin{cases}
\text{die Gleichung (11.) ist hier } 1+10+7=18=\frac{1}{2}(u-1)(v+1)=\frac{1}{2}.6.12,\\
\text{ - - - (12.) - - } 5+7+3=15=\frac{1}{2}(u-1)(v-1)=\frac{1}{2}.6.10,\\
\text{ - - - (13.) - - } 2+8+5=15=\frac{1}{2}(u-1)(v-1)=\frac{1}{2}.6.10,\\
\text{ - - - (14.) - - } 5+10=15=\frac{1}{2}(u-1)(v-1)=\frac{1}{2}.6.10,\\
\text{ - - - (15.) - - } 8+7=15=\frac{1}{2}(u-1)(v-1)=\frac{1}{2}.6.10,\\
\text{ - - - (16.) - - } 2.10-2-3=15=\frac{1}{2}(u-1)(v-1)=\frac{1}{2}.6.10,\\
\text{ - - - (17.) - - } 2+3+5=10;
\end{cases}$$

Alles wie gehörig.

Beweis. *A.* Dafs alle die 8 verschiedenen Classen für die z stattfinden *können*, ist offenbar. Es ist nur zu bemerken, dafs nicht, wie es scheinen könnte, auch noch für (5. Drittens), eben wie (5. Erstlich und Zweitens), ein *dritter* Fall $r=0$ und *zugleich* $\rho=0$, also keine *neunte* Classe möglich ist. Denn könnte ein z mit u und v *zugleich aufgehen*, so würde es, da u und v nach der Voraussetzung zu einander *theilerfremd* sind, zufolge (§. 26.) auch mit dem Product uv *aufgehen* müssen; was nicht möglich ist, da das *gröfste* der z erst $\frac{1}{2}(uv-1)$ ist und also *alle* $z<uv$ sind.

B. Dafs kein z in *mehr als einer* Classe *zugleich* vorkommen kann, ist ebenfalls offenbar; denn eine Zahl z kann zu einer andern u oder v nicht *verschiedene* Reste zugleich lassen. Da nun zugleich jedes z nothwendig in einer der 8 Classen vorkommen *mufs*, indem nicht mehr als die 8 Fälle möglich sind, so folgt, dafs die *Summe* der Mengen der z in den verschiedenen 8 Classen der Anzahl der z *selbst* gleich ist. Diese letztere ist $\frac{1}{2}(uv-1)$, also mufs

$$24.\quad n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8=\tfrac{1}{2}(uv-1)$$

sein. Dies ist die Gleichung (7.) des Lehrsatzes.

C. Die mit u *aufgehenden* z, n_7+n_8 an der Zahl, sind offenbar die *Vielfachen*

$$25.\quad u,\ 2u,\ 3u,\ 4u,\ \ldots\ \tfrac{1}{2}(v-1)u$$

von u, und keine mehr; denn das *nächste* Vielfache von u, nemlich $\frac{1}{2}(v+1)u$, ist schon *gröfser* als der *gröfste* Werth $\frac{1}{2}(uv-1)$ von z. Die Anzahl jener Vielfachen von u (25.) ist aber $\frac{1}{2}(v-1)$, also ist

$$26.\quad n_7+n_8=\tfrac{1}{2}(v-1).$$

Dieses ist die Gleichung (8.) des Lehrsatzes.

D. Die mit v *aufgehenden* z, n_1+n_4 an der Zahl, sind die *Vielfachen*

$$27.\quad v,\ 2v,\ 3v,\ 4v,\ \ldots\ \tfrac{1}{2}(u-1)v$$

von v, und keine mehr; denn das *nächste* Vielfache von v, nemlich $\frac{1}{2}(u+1)v$, ist schon *gröfser* als der *gröfste* Werth $\frac{1}{2}(uv-1)$ von z. Die Anzahl der

Vielfachen von v (27.) ist aber $\frac{1}{2}(u-1)$, also ist

$$28.\quad n_1+n_4=\tfrac{1}{2}(u-1).$$

Dieses ist die Gleichung (9.) des Lehrsatzes.

E. Folgende Zahlen x, und keine anderen, nemlich:

$$29.\ \begin{cases}
\text{Die } \tfrac{1}{2}(u+1) \text{ Zahlen } 1,\ v+1,\ 2v+1,\ 3v+1,\ \ldots\ \tfrac{1}{2}(u-1)v+1 \text{ lassen zu } v \text{ den Rest } 1.\\
\text{Die } \tfrac{1}{2}(u+1) \text{ Zahlen } 2,\ v+2,\ 2v+2,\ 3v+2\ \ldots\ \tfrac{1}{2}(u-1)v+2 \text{ lassen zu } v \text{ den Rest } 2,\\
\text{Die } \tfrac{1}{2}(u+1) \text{ Zahlen } 3,\ v+3,\ 2v+3,\ 3v+3,\ \ldots\ \tfrac{1}{2}(u-1)v+3 \text{ lassen zu } v \text{ den Rest } 3,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\text{Die } \tfrac{1}{2}(u+1) \text{ Zahlen } \tfrac{1}{2}(v-1),\ v+\tfrac{1}{2}(v-1),\ 2v+\tfrac{1}{2}(v-1),\ \ldots\ \tfrac{1}{2}(u-1)v+\tfrac{1}{2}(v-1) \text{ lassen zu } v \text{ den Rest } \tfrac{1}{2}(v-1).
\end{cases}$$

Alle diese Zahlen finden sich unter den Werthen, welche x haben kann; denn die *gröfste* unter ihnen $\frac{1}{2}(u-1)v+\frac{1}{2}(v-1)=\frac{1}{2}(uv-1)$ ist nur eben so grofs als x soll sein können; alle andern sind kleiner. Desgleichen lassen sie *alle* zu v Reste, die $<\frac{1}{2}v$ und >0 sind. Sie sind also zusammengenommen die $n_2+n_3+n_7$ Zahlen x in der 2ten, 5ten und 7ten Classe (6.).

Nun ist die Anzahl der x in (29.) $=\frac{1}{2}(u+1).\frac{1}{2}(v-1)$, denn in jeder horizontalen Reihe stehen $\frac{1}{2}(u+1)$ Zahlen und die Anzahl der Reihe ist $\frac{1}{2}(v-1)$. Also ist

$$30.\quad n_2+n_5+n_7=\tfrac{1}{2}(u+1)\tfrac{1}{2}(v-1).$$

Dieses ist die Gleichung (10.) des Lehrsatzes.

F. Folgende Zahlen x, und keine anderen, nemlich:

$$31.\ \begin{cases}
\text{Die } \tfrac{1}{2}(v+1) \text{ Zahlen } 1,\ u+1,\ 2u+1,\ 3u+1,\ \ldots\ \tfrac{1}{2}(v-1)u+1 \text{ lassen zu } u \text{ den Rest } 1,\\
\text{Die } \tfrac{1}{2}(v+1) \text{ Zahlen } 2,\ u+2,\ 2u+2,\ 3u+2,\ \ldots\ \tfrac{1}{2}(v-1)u+2 \text{ lassen zu } u \text{ den Rest } 2,\\
\text{Die } \tfrac{1}{2}(v+1) \text{ Zahlen } 3,\ u+3,\ 2u+3,\ 3u+3,\ \ldots\ \tfrac{1}{2}(v-1)u+3 \text{ lassen zu } u \text{ den Rest } 3,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\text{Die } \tfrac{1}{2}(v+1) \text{ Zahlen } \tfrac{1}{2}(u-1),\ u+\tfrac{1}{2}(u-1),\ 2u+\tfrac{1}{2}(u-1),\ \ldots\ \tfrac{1}{2}(v-1)u+\tfrac{1}{2}(u-1) \text{ lassen zu } u \text{ den Rest } \tfrac{1}{2}(u-1).
\end{cases}$$

Alle diese Zahlen finden sich unter den Werthen, welche x haben kann; denn die *gröfste* unter ihnen ist $\frac{1}{2}(v-1)u+\frac{1}{2}(u-1)=\frac{1}{2}(uv-1)$, also nur das gröfste x. Alle andern sind kleiner. Auch lassen sie *alle* zu u Reste, die $<\frac{1}{2}u$ und >0 sind. Sie sind also zusammen die $n_4+n_5+n_6$ Zahlen x in der 4ten, 5ten und 6ten Classe (6.).

Die Anzahl der x in (31.) ist aber $\frac{1}{2}(v+1).\frac{1}{2}(u-1)$, denn jede der $\frac{1}{2}(u-1)$ horizontalen Reihen enthält $\frac{1}{2}(v+1)$ Zahlen. Also ist

$$32.\quad n_4+n_5+n_6=\tfrac{1}{2}(u-1)(v+1).$$

Dieses ist die Gleichung (11.) des Lehrsatzes.

G. Die $n_3+n_6+n_8$ Zahlen x in (6.) lassen sämmtlich nach v Reste $\rho>\frac{1}{2}v$. Zieht man $n_1+n_4=\frac{1}{2}(u-1)$ (9.) und $n_2+n_5+n_7=\frac{1}{4}(u+1)(v-1)$ (10.) von $n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8=\frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_3+n_6+n_8 = \tfrac{1}{2}(uv-1)-\tfrac{1}{2}(u-1)-\tfrac{1}{4}(u+1)(v-1) \text{ oder}$$
$$= \tfrac{1}{2}uv-\tfrac{1}{2}-\tfrac{1}{2}u+\tfrac{1}{2}-\tfrac{1}{4}uv+\tfrac{1}{4}u-\tfrac{1}{4}v+\tfrac{1}{4} \text{ oder}$$

$$33. \quad n_3+n_6+n_8 = \tfrac{1}{4}uv-\tfrac{1}{4}u-\tfrac{1}{4}v+\tfrac{1}{4} = \tfrac{1}{4}(u-1)(v-1).$$

Dies ist die Gleichung (12.) des Lehrsatzes.

H. Die $n_1+n_2+n_3$ Zahlen z in (6.) lassen sämmtlich nach u Reste $r>\frac{1}{2}u$. Zieht man $n_7+n_8=\frac{1}{2}(v-1)$ (8.) und $n_4+n_5+n_8=\frac{1}{4}(u-1)(v+1)$ (11.) von $n_1+n_2+n_3+n_4+n_5+n_6+n_7+n_8=\frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_1+n_2+n_3 = \tfrac{1}{2}(uv-1)-\tfrac{1}{2}(v-1)-\tfrac{1}{4}(u-1)(v+1) \text{ oder}$$
$$= \tfrac{1}{2}uv-\tfrac{1}{2}-\tfrac{1}{2}v+\tfrac{1}{2}-\tfrac{1}{4}uv-\tfrac{1}{4}u+\tfrac{1}{4}v+\tfrac{1}{4} \text{ oder}$$

$$34. \quad n_1+n_2+n_3 = \tfrac{1}{4}uv-\tfrac{1}{4}u-\tfrac{1}{4}v+\tfrac{1}{4} = \tfrac{1}{4}(u-1)(v-1).$$

Dies ist die Gleichung (13.) des Lehrsatzes.

I. a. So wie die $\frac{1}{2}(uv-1)$ Zahlen

$$35. \quad 1, 2, 3, 4, \ldots \tfrac{1}{2}(uv-1)$$

durch z bezeichnet wurden, so mögen die *weiter folgenden* $\frac{1}{2}(uv-1)$ Zahlen

$$36. \quad \tfrac{1}{2}(uv+1), \ \tfrac{1}{2}(uv+3), \ \tfrac{1}{2}(uv+5), \ \ldots \ uv-1$$

durch w bezeichnet werden. Alsdann gehört zu *jedem* z ein w, und *nur ein* w, welches mit ihm zusammen uv ausmacht: nemlich 1 mit $uv-1$, 2 mit $uv-2$, 3 mit $uv-3$, ... $\frac{1}{2}(uv-1)$ mit $\frac{1}{2}(uv+1)$ zusammen machen sämmtlich uv aus. Wenn man also in der Gleichung

$$37. \quad z+w = uv$$

dem z *alle* die $\frac{1}{2}(uv-1)$ Werthe (35.), die es haben kann, giebt, so hat w seinerseits *alle* die $\frac{1}{2}(uv-1)$ Werthe (36.), die ihm zukommen.

b. Nun sei für irgend ein z, welches weder mit u noch mit v *aufgeht*, nach (2. u. 3.)

$$38. \quad z = m_1u+r = m_2v+\varrho,$$

wo also weder r noch ϱ Null aber $r<u$, $\varrho<v$ ist. Für das *zugehörige* w sei

$$39. \quad w = \mu_1u+r' = \mu_2v+\varrho',$$

wo $r'<u$ und $\varrho'<v$ angenommen wird; alsdann kann auch weder r' noch ϱ' Null sein. Denn ginge w mit u oder mit v auf, so müfste zufolge (37.) auch z mit u oder mit v aufgehen, gegen die Voraussetzung. Zufolge (37.) ist aus (38. u. 39.)

$$40. \quad z+w = (m_1+\mu_1)u+r+r' = (m_2+\mu_2)v+\varrho+\varrho' = uv.$$

Dieses ist so viel als die *zwei* Gleichungen

$$41. \quad uv = (m_1+\mu_1)u+r+r' \quad \text{und}$$
$$42. \quad uv = (m_2+\mu_2)v+\varrho+\varrho'$$

Aus (41. u. 42.) folgt, dafs $r+r'$ mit u und $\varrho+\varrho'$ mit v *aufgehen* mufs (§. 18.). Aber $r+r'$ ist >0 und $<2u$, weil $r>0<u$ und $r'>0<u$; also mufs nothwendig

$$43. \quad r+r' = u$$

sein; denn zwischen 0 und $2u$ liegt keine andere Zahl als u selbst, die mit u aufginge. Gleichmäfsig ist $\varrho+\varrho'>0$ und $<2v$, weil $\varrho>0<v$ und $\varrho'>0<v$ ist; also mufs auch nothwendig

$$44. \quad \varrho+\varrho' = v$$

sein; aus gleichen Gründen.

Aus (43. u. 44.) folgt nun weiter, dafs, wenn $r>\frac{1}{2}u$ ist, $r'<\frac{1}{2}u>0$ sein mufs, und umgekehrt; desgleichen, dafs, wenn $\varrho>\frac{1}{2}v$ ist, $\varrho'<\frac{1}{2}v>0$ sein mufs, und umgekehrt.

c. Nun sind n_3 Zahlen z vorhanden, für welche $r>\frac{1}{2}u$ und *zugleich* $\varrho>\frac{1}{2}v$ ist (6.), also mufs es *eben so viele* Zahlen w geben, für welche $r'<\frac{1}{2}u>0$ und *zugleich* $\varrho'<\frac{1}{2}v>0$ ist, denn zu jedem z gehört ein w, für welches $r'<\frac{1}{2}u>0$ und $\varrho'<\frac{1}{2}v>0$, wenn für das zugehörige z, $r>\frac{1}{2}u$ und $\varrho>\frac{1}{2}v$ ist (6.).

Desgleichen sind n_5 Zahlen z vorhanden, für welche $r<\frac{1}{2}u>0$ und *zugleich* $\varrho<\frac{1}{2}v>0$ ist (6.), also mufs es *eben so viele* Zahlen w geben, für welche $r'>u$ und *zugleich* $\varrho'>\frac{1}{2}v$ ist; aus gleichen Gründen.

Es sind also unter den Zahlen z und w *zusammengenommen*, das heifst unter den Zahlen

$$45. \quad 1, 2, 3, 4, \ldots \, uv-1$$

nothwendig überhaupt n_3+n_5 Zahlen vorhanden, die, weder mit u noch mit v *aufgehend*, nach u Reste r oder $r'>\frac{1}{2}u$ und *zugleich* nach v Reste ϱ *oder* $\varrho'>\frac{1}{2}v$ lassen; und *eben so viele* Zahlen, welche, weder mit u noch mit v *aufgehend*, nach u Reste r *oder* $r'<\frac{1}{2}u>0$ und *zugleich* nach v Reste ϱ *oder* $\varrho'<\frac{1}{2}v>0$ lassen.

d. Um durch u und v ausgedrückt zu finden, wie viele solcher letztgenannten Zahlen unter den z und w zusammengenommen sich befinden, bezeichne x jede derjenigen Zahlen aus der *Gesammtheit* der z und w, also aus den Zahlen (45.), welche mit u dividirt einen Rest $\varepsilon<\frac{1}{2}u>0$ und mit v dividirt einen Rest $\sigma<\frac{1}{2}v>0$ läfst; so dafs also

$$46. \quad x = eu+\varepsilon = sv+\sigma$$

ist, wo $\varepsilon<\frac{1}{2}u>0$, *zugleich* $\sigma<\frac{1}{2}v>0$ und $x<uv$ also $e<v$, $s<u$ sein soll.

e. Aus (46.) folgt

$$47. \quad sv = eu + \varepsilon - \sigma.$$

In dieser Gleichung soll also ε alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(u-1)$ und σ alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(v-1)$ bekommen können, während $s < u$, $e < v$ ist. Was nun auch $\varepsilon - \sigma$ sein mag, positiv, oder negativ, oder Null: immer giebt es nach (§. 34. III.) einen Werth von $s < u$, welcher der Gleichung (47.) genug thut; also kann in (47.) und folglich in (46.) in der That $s < u$ und folglich, da σ nothwendig $< v$ ist, auch $x < uv$ sein. Also kann in (46.) ε wirklich alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(u-1)$ und σ alle die Werthe $1, 2, 3, \ldots \frac{1}{2}(v-1)$ haben, für $x < uv$.

f. Nun kann zunächst in (46.) erst ε ohne Rücksicht auf $sv + \sigma$ offenbar alle die Werthe $1, 2, 3, 4, \ldots \frac{1}{2}(u-1)$ haben; denn *alle* die x, welche diese Werthe des Restes ε geben, sind *vorhanden*.

Aber giebt man dem ε irgend einen *bestimmten* Werth, z. B. 1, so kann zufolge (*e.*) für dieses *nemliche* $\varepsilon = 1$, σ jeden der $\frac{1}{2}(v-1)$ Werthe $1, 2, 3, \ldots \frac{1}{2}(v-1)$ haben, und zwar offenbar immer für ein *anderes* x, da ein und dasselbe x nicht verschiedene Reste σ lassen kann. Für $\varepsilon = 1$ findet sich also zu jedem $\sigma = 1, 2, 3, \ldots \frac{1}{2}(v-1)$ irgend ein x. Folglich giebt es in (46.) $\frac{1}{2}(v-1)$ *verschiedene* x, die alle den Rest $\varepsilon = 1$, aber die *verschiedenen* Reste $\sigma = 1, 2, 3, \ldots \frac{1}{2}(v-1)$ lassen.

Ganz gleich verhält es sich für *jeden* der $\frac{1}{2}(u-1)$ Werthe $1, 2, 3, \ldots$ $\ldots \frac{1}{2}(u-1)$, welche ε haben kann.

Also giebt es überhaupt $\frac{1}{2}(u-1) \cdot \frac{1}{2}(v-1) = \frac{1}{4}(u-1)(v-1)$ verschiedene x unter den Zahlen (45.), welche nach u Reste $< \frac{1}{2}u > 0$ und *zugleich* nach v Reste $< \frac{1}{2}v > 0$ lassen. Die Anzahl dieser Zahlen war (*c.*) $= n_3 + n_5$, also ist

$$48. \quad n_3 + n_5 = \tfrac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (14.) des Lehrsatzes.

K. Zieht man $n_7 + n_8 = \frac{1}{2}(v-1)$ (8.), $n_1 + n_4 = \frac{1}{2}(u-1)$ (9.) und $n_3 + n_5 = \frac{1}{4}(u-1)(v-1)$ (14.) von $n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_2 + n_6 = \tfrac{1}{2}(uv-1) - \tfrac{1}{2}(v-1) - \tfrac{1}{2}(u-1) - \tfrac{1}{4}(u-1)(v-1) \text{ oder}$$

$$n_2 + n_6 = \tfrac{1}{2}uv - \tfrac{1}{2} - \tfrac{1}{2}v + \tfrac{1}{2} - \tfrac{1}{2}u + \tfrac{1}{2} - \tfrac{1}{4}uv + \tfrac{1}{4}u + \tfrac{1}{4}v - \tfrac{1}{4} \text{ oder}$$

$$49. \quad n_2 + n_6 = \tfrac{1}{4}uv - \tfrac{1}{4}u - \tfrac{1}{4}v + \tfrac{1}{4} = \tfrac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (15.) des Lehrsatzes.

L. Addirt man $n_2+n_6=\frac{1}{4}(u-1)(v-1)$ (15.) zu $2(n_3+n_5)=\frac{1}{4}(u-1)(v-1)$ (14.) und zieht von der Summe $n_2+n_6+n_8=\frac{1}{4}(u-1)(v-1)$ (12.) und $n_1+n_2+n_3=\frac{1}{4}(u-1)(v-1)$ (13.) ab, so ergiebt sich
$2(n_3+n_5)+n_2+n_6-n_3-n_6-n_8-n_1-n_2-n_3=(\frac{1}{4}+\frac{1}{4}-\frac{1}{4}-\frac{1}{4})(u-1)(v-1)$ oder

$$50. \quad 2n_5-n_1-n_8=\tfrac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (16.) des Lehrsatzes.

M. Zieht man endlich $n_3+n_5=\frac{1}{4}(u-1)(v-1)$ (14.) von $2n_5-n_1-n_8=\frac{1}{4}(u-1)(v-1)$ (16.) ab, so ergiebt sich

$$2n_5-n_1-n_8-n_3-n_5=0 \text{ oder}$$

$$51. \quad n_1+n_8+n_3=n_5.$$

Dieses ist die Gleichung (17.) des Lehrsatzes.

N. Anm. Der Theil des Beweises (*L.*) enthält eigenthümliche Erwägungen und bedarf wesentlich des Satzes (§. 34.), welcher auch weiterhin oft nöthig ist. Alles Übrige ist sehr einfach.

§. 37.

Lehrsatz.

I. *Es seien* m *und* n *zwei beliebige positive ganze Zahlen und es sei*

$$1. \quad n>m.$$

Setzt man

$$2. \begin{cases} m=\mu_1 n+r_1, \\ 2m=\mu_2 n+r_2, \\ 3m=\mu_3 n+r_3, \\ \dots\dots \\ (n-1)m=\mu_{n-1}n+r_{n-1}, \\ nm=\mu_n n+r_n, \end{cases} \quad \textit{und} \quad 3. \begin{cases} n=\nu_1 m+\varrho_1, \\ 2n=\nu_2 m+\varrho_2, \\ 3n=\nu_3 m+\varrho_3, \\ \dots\dots \\ (m-1)n=\nu_{m-1}m+\varrho_{m-1}, \\ mn=\nu_m m+\varrho_m \end{cases}$$

unter der Bedingung, dafs die sämmtlichen r *und* ϱ *positiv sind und*

$$4. \quad \textit{die } r \textit{ aus den Zahlen } 1, 2, 3, 4, \dots n,$$

$$5. \quad \textit{die } \varrho \textit{ aus den Zahlen } 0, 1, 2, 3, \dots m-1$$

genommen werden, und bezeichnet die Summe der sämmtlichen Quotienten μ, *nemlich*

$$6. \quad \mu_1+\mu_2+\mu_3\dots+\mu_{n-1}+\mu_n \textit{ durch } S\mu;$$

die Summe der sämmtlichen Quotienten ν, *nemlich*

$$7. \quad \nu_1+\nu_2+\nu_3\dots+\nu_{m-1}+\nu_m \textit{ durch } S\nu;$$

die Summe der sämmtlichen Reste r, nemlich

$$8. \quad r_1+r_2+r_3\dots+r_{n-1}+r_n \textit{ durch } Sr;$$

die Summe der sämmtlichen Reste ϱ, *nemlich*

$$9.\quad \varrho_1+\varrho_2+\varrho_3\;\ldots\ldots+\varrho_{m-1}+\varrho_m \text{ durch } S\varrho,$$

so ist

$$10.\quad r_n = n,\quad \varrho_m = 0,$$

$$11.\quad \mu_n = m-1 \text{ und } \nu_m = n,$$

$$12.\quad S\mu+S\nu = mn,$$

$$13.\quad mSr+nS\varrho = \tfrac{1}{2}mn(m+n).$$

II. *Sind* m *und* n *zu einander theilerfremd, so ist*

$$14.\quad Sr = \tfrac{1}{2}n(n+1),$$

$$15.\quad S\varrho = \tfrac{1}{2}m(m-1),$$

$$\left.\begin{array}{l}16.\quad S\mu = \tfrac{1}{2}(n+1)(m-1)\\ 17.\quad S\nu = \tfrac{1}{2}((n-1)m+n+1)\end{array}\right\} S\mu+S\nu=mn,$$

$$18.\quad S\mu-\mu_n = S\nu-\nu_m = \tfrac{1}{2}(n-1)(m-1).$$

Beispiel 1. Es sei für *beliebige* m und n,

$$19.\quad m = 8,\quad n = 20,$$

so ist in (2 u. 3.)

$$20.\ \left\{\begin{array}{rcl} 1,\ 2m &=& 0n+8,\ 16,\\ 3,\ 4,\ 5m &=& 1n+4,\ 12,\ 20,\\ 6,\ 7m &=& 2n+8,\ 16,\\ 8,\ 9,\ 10m &=& 3n+4,\ 12,\ 20,\\ 11,\ 12m &=& 4n+8,\ 16,\\ 13,\ 14,\ 15m &=& 5n+4,\ 12,\ 20,\\ 16,\ 17m &=& 6n+8,\ 16,\\ 18,\ 19,\ 20m &=& 7n+4,\ 12,\ 20,\end{array}\right. \quad\text{und}\quad 21.\ \left\{\begin{array}{rcl} 1n &=& 2m+4,\\ 2n &=& 5m+0,\\ 3n &=& 7m+4,\\ 4n &=& 10m+0,\\ 5n &=& 12m+4,\\ 6n &=& 15m+0,\\ 7n &=& 17m+4,\\ 8n &=& 20m+0.\end{array}\right.$$

Die Summe *aller* Quotienten μ und ν ist hier

$$S\mu+S\nu=2.0+3.1+2.2+3.3+2.4+3.5+2.6+3.7+2+5+7+10+12+15+17+20,\ \text{oder}$$

$$22.\quad S\mu+S\nu=3+4+9+8+15+12+21+88=160=8.20=mn;$$

gemäfs (12.). Ferner ist

$$23.\quad \mu_n = 7 = m-1 \text{ und } \nu_m = 20 = n; \text{ gemäfs (11.)},$$

$$24.\quad mSr+nS\varrho = 8(8+16+4+12+20)4+20.4.4 = 4.8.60+320 = 2240 = \tfrac{1}{2}.8.20(8+20) = \tfrac{1}{2}mn(m+n); \text{ gemäfs (13.)},$$

$$25.\quad r_n = 20 = n \text{ und } \varrho_m = 0; \text{ gemäfs (10.)}.$$

Beispiel 2. Es sei für *theilerfremde* m und n,

$$26.\quad m = 9,\quad n = 38,$$

so ist in (2. u. 3.)

27.
$$\begin{cases} 1,\ 2,\ 3,\ 4m = 0n+9,\ 18,\ 27,\ 36, \\ 5,\ 6,\ 7,\ 8m = 1n+7,\ 16,\ 25,\ 34, \\ 9,\ 10,\ 11,\ 12m = 2n+5,\ 14,\ 23,\ 32, \\ 13,\ 14,\ 15,\ 16m = 3n+3,\ 12,\ 21,\ 30, \\ 17,\ 18,\ 19,\ 20,\ 21m = 4n+1,\ 10,\ 19,\ 28,\ 37, \\ 22,\ 23,\ 24,\ 25m = 5n+8,\ 17,\ 26,\ 35, \\ 26,\ 27,\ 28,\ 29m = 6n+6,\ 15,\ 24,\ 33, \\ 30,\ 31,\ 32,\ 33m = 7n+4,\ 13,\ 22,\ 31, \\ 34,\ 35,\ 36,\ 37,\ 38m = 8n+2,\ 11,\ 20,\ 29,\ 38, \end{cases}$$

28.
$$\begin{cases} 1n = 4m+2, \\ 2n = 8m+4, \\ 3n = 12m+6, \\ 4n = 16m+8, \\ 5n = 21m+1, \\ 6n = 25m+3, \\ 7n = 29m+5, \\ 8n = 33m+7, \\ 9n = 38m+0. \end{cases}$$

Die Summe der Quotienten μ und ν ist hier

$$S\mu = 4.0+4.1+4.2+4.3+5.4+4.5+4.6+4.7+5.8 \quad \text{oder}$$

29. $$S\mu = 4+8+12+20+20+24+28+40 = 156 = \tfrac{1}{2}(38+1)(9-1) = \tfrac{1}{2}.39.8 = \tfrac{1}{2}(n+1)(m-1); \text{ gemäfs (16.)}.$$

Die Summe der Quotienten ν ist

30. $$S\nu = 4+8+12+16+21+25+29+33+38 = 186 = \tfrac{1}{2}((38-1).9+38+1) = \tfrac{1}{2}(37.9+39) = 186 = \tfrac{1}{2}((n-1)m+n+1);$$

gemäfs (17.). Ferner ist

31. $$S\mu-\mu_n = 156-8 = S\nu-\nu_m = 186-38 = 148 = \tfrac{1}{2}.37.8 = \tfrac{1}{2}(n-1)(m-1); \text{ gemäfs (18.)},$$

32. $$Sr = (1+2+3\ldots.+38) = \tfrac{1}{2}.38.39 = \tfrac{1}{2}n(n+1); \text{ gemäfs (14.)},$$

33. $$S\varrho = (1+2+3\ldots.+\ 8) = \tfrac{1}{2}.\ 8.\ 9 = \tfrac{1}{2}m(m-1); \text{ gemäfs (15.)}.$$

Beweis. *A.* Da $m<n$ sein soll und zufolge der *ersten* Gleichung (3.) $\nu_1 m$ noch um ϱ_1 kleiner als n ist, so ist in (2.) für m, $2m$, $3m$, ... $\nu_1 m$ nothwendig $\mu_1 = 0$. Also sind die *ersten* ν_1 Quotienten μ_1, μ_2, μ_3, ... μ_{ν_1} sämmtlich Null.

Das nächstfolgende Vielfache $(\nu_1+1)m$ von m ist schon $>n$; denn, noch einmal m zu der ersten Gleichung (3.) gethan, würde einen Rest ϱ_1+m geben, der $>m$ wäre; was nicht sein soll. Also ist der Quotient μ_{ν_1+1} in (2.) der *erste* derjenigen, welche *nicht Null*, sondern 1 sind. Aber $\nu_2 m$ ist nach der 2ten Gleichung in (3.) noch um ϱ_2 kleiner als $2n$ Also sind in (2.) auch alle folgenden Vielfachen $(\nu_1+2)m$, $(\nu_1+3)m$, $(\nu_1+4)m$ etc., von m bis zu $\nu_2 m$, noch kleiner als $2n$, und folglich sind alle die $\nu_2-\nu_1$ Quotienten μ_{ν_1+1}, μ_{ν_1+2}, μ_{ν_1+3}, ... μ_{ν_2} in (2.) sämmtlich $=1$.

Auf dieselbe Weise folgt, dafs die sämmtlichen $\nu_3-\nu_2$ Quotienten μ_{ν_2+1}, μ_{ν_2+2}, ν_{ν_2+3}, ... μ_{ν_3} in (2.) $=2$ sind, die sämmtlichen $\nu_4-\nu_3$ Quo-

tienten $\mu_{\nu_3+1}, \mu_{\nu_3+2}, \mu_{\nu_3+3}, \ldots \mu_{\nu_4}$ in (2.) $= 3$; u. s. w. Zuletzt also sind die letzten $\nu_m - \nu_{m-1}$ Quotienten μ gleich $m-1$.

B. Nimmt man dieses zusammen, so ergiebt sich Folgendes:

34.
$$\begin{cases} \text{die ersten } \nu_1 \text{ Quotienten } \mu \text{ sind } = 0, \\ \text{die folgenden } \nu_2-\nu_1 \text{ Quotienten } \mu \text{ sind } = 1, \\ \text{die folgenden } \nu_3-\nu_2 \text{ Quotienten } \mu \text{ sind } = 2, \\ \ldots\ldots\ldots\ldots\ldots \\ \text{die vorletzten } \nu_{m-1}-\nu_{m-2} \text{ Quotienten } \mu \text{ sind } = m-2, \\ \text{die letzten } \nu_m - \nu_{m-1} \text{ Quotienten } \mu \text{ sind } = m-1. \end{cases}$$

Der Betrag $S\mu$ der *sämmtlichen Quotienten* μ (6.) ist also

35. $$S\mu = 0\nu_1 + 1(\nu_2-\nu_1) + 2(\nu_3-\nu_2) + 3(\nu_4-\nu_3) \ldots \ldots + (m-2)(\nu_{m-1}-\nu_{m-2}) + (m-1)(\nu_m-\nu_{m-1}).$$

Daraus folgt, wenn man wegläfst was sich aufhebt,

$$S\mu = -\nu_1 - \nu_2 - \nu_3 - \nu_4 \ldots - \nu_{m-1} + (m-1)\nu_m = -S\nu + m\nu_m \quad (7.) \text{ oder}$$

36. $$S\mu + S\nu = m\nu_m.$$

C. Nun ist in der *letzten* Gleichung (3.) $\nu_m = n$, und in der letzten Gleichung (2.) $\mu_n = m-1$. Denn es kann in $mn = \nu_n m + \varrho_m$ der Rest ϱ_m nur $=0$ oder $=m$ sein, weil $\nu_m m$ mit m *aufgeht* und also auch ϱ_m mit m aufgehen mufs; eben so kann in $nm = \mu_n n + r_n$ der Rest r_n nur $= 0$ oder $= n$ sein, weil $\mu_n n$ mit n aufgeht und also auch r_n mit n aufgehen mufs. Aber ein $\varrho = m$ *soll* nach (5.) und ein $r = 0$ nach (4.) nicht Statt finden. Also kann in der letzten Gleichung (3.) ϱ_m *nur* $= 0$ und folglich r_m *nur* $= n$ sein, wie es (10.) behauptet, und in der letzten Gleichung (2.) kann r_m *nur* $= n$ und folglich μ_n *nur* $= m-1$ sein, wie es (11.) behauptet.

D. Setzt man dem gemäfs in (36.) für ν_m seinen Werth n, so ergiebt sich

37. $$S\mu + S\nu = mn;$$

welches die Gleichung (12.) des Lehrsatzes ist.

E. Summirt man alle die Gleichungen (2.), so wie diejenigen (3.), so erhält man

38. $$(1+2+3+4 \ldots + n)m = nS\mu + Sr = \tfrac{1}{2}(n+1)nm \text{ und}$$

39. $$(1+2+3+4 \ldots + m)n = mS\nu + S\varrho = \tfrac{1}{2}(m+1)mn.$$

In (38.) mit m und in (39.) mit n multiplicirt und die Summe der Producte genommen, giebt

40. $$\tfrac{1}{2}mn(n+1)m + \tfrac{1}{2}mn(m+1)n = mn(S\mu + S\nu) + mSr + nS\varrho,$$

oder, da $S\mu + S\nu = mn$ ist (12.),

$$\tfrac{1}{2}mn[m(n+1)+n(m+1)] = m^2n^2+mSr+nS\varrho \text{ oder}$$

$$41. \quad mSr+nS\varrho = \tfrac{1}{2}mn(m+n);$$

welches die Gleichung (13.) des Lehrsatzes ist.

F. Sind m und n zu einander *theilerfremd,* so sind nach (§. 34.) in (2.) die r die sämmtlichen Zahlen

$$42. \quad 1,\ 2,\ 3,\ 4,\ \ldots\ n-1,\ n.$$

Denn nach (§. 34. I.) würden in (2.) den Factoren 0, 1, 2, 3, ... $n-1$ von m die Reste 0, 1, 2, 3, 4, .. . $n-1$ zukommen, und zu dem Reste 0 gehört der Factor 0 (§. 34. I.). Dieser Factor 0 findet hier nicht Statt, also auch nicht der Rest 0. Dagegen kommt hier der Factor n noch hinzu, und für diesen ist der Rest r zufolge (10.) $=n$. Also sind die r in (2.) nothwendig alle die Zahlen (42.).

Eben so sind die ϱ in (3.) die sämmtlichen Zahlen

$$43. \quad 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ m-1.$$

Denn den Factoren 1, 2, 3, ... $m-1$ in (3.) kommen nach (§. 34. I.) die Reste 1, 2, 3, ... $n-1$ zu, und der zu dem letzten Factor m in (3.) gehörige Rest ϱ_m ist nach (10.) $=0$, so dafs also zusammen die ϱ die Zahlen (43.) sind.

G. Aus (42. und 43.) folgt nun unmittelbar, dafs die Summe der Reste r, nemlich Sr, $=\frac{1}{2}(n+1)n$ und die Summe der Reste ϱ, nemlich $S\varrho$, $=\frac{1}{2}m(m-1)$ ist; wie es (14. u. 15.) behaupten.

H. Setzt man (14. u. 15.) in die Gleichungen (38. u. 39.), welche hier in dem besonderen Fall ebenfalls stattfinden, da sie für *jedes* m und n allgemein gelten; so ergiebt sich

$$44. \quad \tfrac{1}{2}(n+1)mn = nS\mu+\tfrac{1}{2}n(n+1) \text{ und}$$

$$45. \quad \tfrac{1}{2}(m+1)mn = mS\nu+\tfrac{1}{2}m(m-1)$$

oder

$$46. \quad \tfrac{1}{2}m(n+1)-\tfrac{1}{2}(n+1) = S\mu = \tfrac{1}{2}(n+1)(m-1) \text{ und}$$

$$47. \quad \tfrac{1}{2}n(m+1)-\tfrac{1}{2}(m-1) = S\nu = \tfrac{1}{2}((n-1)m+n+1);$$

welches die Gleichungen (16. u. 17.) des Lehrsatzes sind.

J. Aus (16, 17. u. 11.) ergiebt sich

$$48. \quad S\mu-\mu_n = \tfrac{1}{2}(n+1)(m-1)-(m-1) = \tfrac{1}{2}(n-1)(m-1) \text{ und}$$

$$49. \quad S\nu-\nu_m = \tfrac{1}{2}(n-1)m+\tfrac{1}{2}(n+1)-n = \tfrac{1}{2}(n-1)(m-1);$$

wie es der Lehrsatz in (18.) behauptet.

K. Anm. Der Beweis erhält seine Entwicklung besonders durch die Summirung der Gleichungen (34. in *B.*), die ihrerseits aus einfachen Be-

trachtungen hervorgehen. In (*E.*) wird der bekannte Ausdruck der Summe einer sogenannten arithmetischen Reihe zu Hülfe genommen.

§. 38.
Lehrsatz.

Es seien m *und* n *zwei beliebige positive ganze Zahlen und es sei*

$$1.\quad n > m.$$

Man setze

$$2.\ \begin{cases} m = \mu_1 n + r_1, \\ 2m = \mu_2 n + r_2, \\ 3m = \mu_3 n + r_3, \\ \dots\dots\dots \\ \frac{1}{2}(n-1)m = \mu_{\frac{1}{2}(n-1)} n + r_{\frac{1}{2}(n-1)}, \\ \text{wenn n ungerade und} \\ \frac{1}{2}nm = \mu_{\frac{1}{2}n} n + r_{\frac{1}{2}n}, \\ \text{wenn n gerade ist,} \end{cases} \quad \text{und}\quad 3.\ \begin{cases} n = \nu_1 m + \rho_1, \\ 2n = \nu_2 m + \rho_2, \\ 3n = \nu_3 m + \rho_3, \\ \dots\dots\dots \\ \frac{1}{2}(m-1)n = \nu_{\frac{1}{2}(m-1)} m + \rho_{\frac{1}{2}(m-1)}, \\ \text{wenn m ungerade und} \\ \frac{1}{2}mn = \nu_{\frac{1}{2}m} m + \rho_{\frac{1}{2}m}, \\ \text{wenn m gerade ist,} \end{cases}$$

unter der Bedingung, dafs die sämmtlichen r *und* ρ *positiv sind und dafs*

4. *die* r *aus den Zahlen* 1, 2, 3, 4, ... n *und*

5. *die* ρ *aus den Zahlen* 0, 1, 2, 3, ... m—1

genommen werden. Ferner bezeichne man die Summe der sämmtlichen Quotienten μ, *nemlich*

6. $\mu_1+\mu_2+\mu_3 \dots\dots + \mu_{\frac{1}{2}(n-1)}$ *oder* $\mu_{\frac{1}{2}n}$ *durch* $S\mu$,

und die Summe der sämmtlichen Quotienten ν, *nemlich*

7. $\nu_1+\nu_2+\nu_3 \dots\dots \nu_{\frac{1}{2}(m-1)}$ *oder* $\nu_{\frac{1}{2}m}$ *durch* $S\nu$.

Alsdann ist

$$8.\ \begin{cases} 1.\ S\mu+S\nu = \frac{1}{4}(m-1)(n-1), \\ 2.\ \mu_{\frac{1}{2}(n-1)} = \frac{1}{2}(m-1) \text{ und } r_{\frac{1}{2}(n-1)} = \frac{1}{2}(n-m); \end{cases} \text{ wenn m ungerade und n ungerade ist;}$$

$$9.\ \begin{cases} 1.\ S\mu+S\nu = \frac{1}{4}(m-1)n, \\ 2.\ \mu_{\frac{1}{2}(n-1)} = \frac{1}{2}(m-1) \text{ und } r_{\frac{1}{2}n} = \frac{1}{2}n; \end{cases} \text{ wenn m ungerade und n gerade ist;}$$

$$10.\ \begin{cases} 1.\ S\mu+S\nu = \frac{1}{4}m(n-1), \\ 2.\ \begin{cases} \mu_{\frac{1}{2}(n-1)} = \frac{1}{2}m-1 \text{ und } r_{\frac{1}{2}(n-1)} = n-\frac{1}{2}m, \\ \nu_{\frac{1}{2}m} = \frac{1}{2}(n-1) \text{ und } \rho_{\frac{1}{2}m} = \frac{1}{2}m; \end{cases} \end{cases} \text{ wenn m gerade und n ungerade ist;}$$

$$11.\ \begin{cases} 1.\ S\mu+S\nu = \frac{1}{4}mn, \\ 2.\ \begin{cases} \mu_{\frac{1}{2}n} = \frac{1}{2}m-1 \text{ und } r_{\frac{1}{2}n} = n, \\ \nu_{\frac{1}{2}m} = \frac{1}{2}n \text{ und } \rho_{\frac{1}{2}m} = 0, \end{cases} \end{cases} \text{ wenn m gerade und n gerade ist.}$$

Beispiel 1. für (8.). Es sei

$$12.\quad m=7,\quad n=35,$$

so geben (2. u. 3.)

$$13.\ \begin{cases} 1,\ 2,\ 3,\ 4,\ 5m=0n+7,\ 14,\ 21,\ 28,\ 35,\\ 6,\ 7,\ 8,\ 9;\ 10m=1n+7,\ 14,\ 21,\ 28,\ 35,\\ 11,\ 12,\ 13,\ 14,\ 15m=2n+7,\ 14,\ 21,\ 28,\ 35,\\ \qquad 16,\ 17m=3n+7,\ 14; \end{cases} \text{ und } 14.\ \begin{cases} 1.35=\ 5.7+0,\\ 2.35=10.7+0,\\ 3.35=15.7+0; \end{cases}$$

und die Summe sämmtlicher Quotienten ist

$$14.\quad S\mu+S\nu=5.0+5.1+5.2+2.3+5+10+15=51=\tfrac{1}{4}(7-1)(35-1)$$
$$=\frac{6.34}{4};\ \text{gemäfs (8. 1.).}$$

Desgleichen ist $\mu_{\frac12(n-1)}=3=\frac12(m-1)$ und $r_{\frac12(n-1)}=14=\frac12(n-m)$; gemäfs (8. 2.).

Beispiel 2. für (8.). Es sei

$$15.\quad m=9,\quad n=39,$$

so geben (2. u. 3.)

$$17.\ \begin{cases} 1,\ 2,\ 3,\ 4m=0n+9,\ 18,\ 27,\ 36,\\ 5,\ 6,\ 7,\ 8m=1n+6,\ 15,\ 24,\ 33,\\ 9,\ 10,\ 11,\ 12,\ 13m=2n+3,\ 12,\ 21,\ 30,\ 39,\\ 14,\ 15,\ 16,\ 17m=3n+9,\ 18,\ 27,\ 36,\\ \qquad 18,\ 19m=4n+6,\ 15; \end{cases} \quad 18.\ \begin{cases} 1.39=\ 4.9+3,\\ 2.39=\ 8.9+6,\\ 3.39=13.9+0,\\ 4.39=17.9+3; \end{cases}$$

also ist die Summe sämmtlicher Quotienten hier

$$19.\quad S\mu+S\nu=4.0+4.1+5.2+4.3+2.4+4+8+13+17=76$$
$$=\tfrac{1}{4}(9-1)(39-1)=\frac{8.38}{4};\ \text{gemäfs (8. 1.).}$$

Desgleichen ist $\mu_{\frac12(n-1)}=4=\frac12(m-1)$ und $r_{\frac12 n}=15=\frac12(n-m)$; gemäfs (8. 2.).

Beispiel 3. für (9.). Es sei

$$20.\quad m=21,\quad n=24,$$

so ist

$$21.\ \left\{\begin{aligned} 1m &= 0n+21,\\ 2m &= 1n+18,\\ 3m &= 2n+15,\\ 4m &= 3n+12,\\ 5m &= 4n+\ 9,\\ 6m &= 5n+\ 6,\\ 7m &= 6n+\ 3,\\ 8m &= 6n+24,\\ 9m &= 7n+21,\\ 10m &= 8n+18,\\ 11m &= 9n+15,\\ 12m &= 10n+12, \end{aligned}\right. \quad \text{und} \quad 22.\ \left\{\begin{aligned} 1n &= 1m+\ 3,\\ 2n &= 2m+\ 6,\\ 3n &= 3m+\ 9,\\ 4n &= 4m+12,\\ 5n &= 5m+15,\\ 6n &= 6m+18,\\ 7n &= 8m+\ 0,\\ 8n &= 9m+\ 3,\\ 9n &= 10m+\ 6,\\ 10n &= 11m+\ 9, \end{aligned}\right.$$

also ist hier

$$23.\quad S\mu+S\nu=61+59=120=\tfrac{1}{4}(21-1)24=\frac{20.24}{4};\ \text{gemäfs (9. 1.).}$$

Desgleichen ist $\mu_{\frac{1}{2}(n-1)}=10=\frac{1}{2}(m-1)$, $r_{\frac{1}{2}(n-1)}=12=\frac{1}{2}n$; gemäfs (9. 2.).

Beispiel 4. für (10.). Es sei

$$24.\quad m=6,\quad n=15,$$

so ist

$$25.\ \left\{\begin{aligned} 1,\ 2m &= 0n+6,\ 12,\\ 3,\ 4,\ 5m &= 1n+3,\ \ 9,\ 15,\\ 6,\ 7m &= 2n+6,\ 12, \end{aligned}\right. \quad \text{und} \quad 26.\ \left\{\begin{aligned} 1n &= 2m+3,\\ 2n &= 5m+0,\\ 3n &= 7m+3, \end{aligned}\right.$$

also ist hier

$$27.\quad S\mu+S\nu=2.0+3.1+2.2+2+5+7=21=\tfrac{1}{4}6(15-1)=\frac{6.14}{4};$$

gemäfs (10. 1.). Desgleichen ist $\mu_{\frac{1}{2}(n-1)}=2=\frac{1}{2}m-1$, $r_{\frac{1}{2}(n-1)}=12=n-\frac{1}{2}m$, $\nu_{\frac{1}{2}m}=7=\frac{1}{2}(n-1)$, $\varrho_{\frac{1}{2}m}=3=\frac{1}{2}m$; gemäfs (10. 2.).

Beispiel 5. für (11.). Es sei

$$28.\quad m=8,\quad n=34,$$

so ist

$$29.\ \left\{\begin{aligned} 1,\ 2,\ 3,\ 4m &= 0n+8,\ 16,\ 24,\ 32,\\ 5,\ 6,\ 7,\ 8m &= 1n+6,\ 14,\ 22,\ 30,\\ 9,\ 10,\ 11,\ 12m &= 2n+4,\ 12,\ 20,\ 28,\\ 13,\ 14,\ 15,\ 16,\ 17m &= 3n+2,\ 10,\ 18,\ 26,\ 34; \end{aligned}\right. \quad \text{und} \quad 30.\ \left\{\begin{aligned} 1n &= 4m+2,\\ 2n &= 8m+4,\\ 3n &= 12m+6,\\ 4n &= 17m+0, \end{aligned}\right.$$

also ist hier

$$31.\quad S\mu+S\nu=4.0+4.1+4.2+5.3+4+8+12+17=68=\tfrac{1}{4}.8.34;$$

gemäfs (11. 1.). Desgleichen ist $\mu_{\frac{1}{2}n}=3=\frac{1}{2}m-1$, $r_{\frac{1}{2}n}=34=n$, $\nu_{\frac{1}{2}m}=17=\frac{1}{2}n$ und $\varrho_{\frac{1}{2}m}=0$; gemäfs (11. 2.).

Beweis. ***Erster Fall*** (8.), ***wenn*** m ***ungerade und*** n ***ungerade ist.*** ***A.*** Ganz wie in dem Beweise (§. 37. *A.*) folgt, dafs die ersten ν_1 Quotienten μ in (2.) Null, die folgenden $\nu_2-\nu_1$ Quotienten $\mu=1$, die folgenden $\nu_3-\nu_2$ Quotienten $\mu=2$ sind, u. s. w.; zuletzt die $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten $=\frac{1}{2}(m-3)$.

B. Nun ist für die *letzte* der Gleichungen (2.), nemlich für die Gleichung $\frac{1}{2}(n-1)m=\mu_{\frac{1}{2}(n-1)}n+r_{\frac{1}{2}(n-1)}$,

32. $\quad \frac{1}{2}(n-1)m = \frac{1}{2}mn-\frac{1}{2}m = \frac{1}{2}(m-1)n+\frac{1}{2}(n-m).$

Hier ist $\frac{1}{2}(n-m)>0$, weil $n>m$ sein soll (1.) und $\frac{1}{2}(n-m)<n$. Auch ist $\frac{1}{2}(n-m)-n=-\frac{1}{2}(n+m)<0$ und $\frac{1}{2}(n-m)+n>n$. Also ist $\frac{1}{2}(n-m)$ der Rest $r_{\frac{1}{2}(n-1)}$, und folglich auch $\frac{1}{2}(m-1)$ aus (32.) der Quotient $\mu_{\frac{1}{2}(n-1)}$, so dafs also

33. $\quad \mu_{\frac{1}{2}(n-1)}=\frac{1}{2}(m-1) \quad$ und $\quad r_{\frac{1}{2}(n-1)}=\frac{1}{2}(n-m)$

ist; wie es (8. 2.) behauptet.

C. Zufolge (*A.*) waren die letzten $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten $\mu=\frac{1}{2}(m-3)$: also auch der $\nu_{\frac{1}{2}(m-1)}$ Quotient μ ist erst $=\frac{1}{2}(m-3)$, und folglich um 1 kleiner als der *letzte* $\mu_{\frac{1}{2}(n-1)}$ der überhaupt vorhandenen $\frac{1}{2}(n-1)$ Quotienten, welcher nach (33.) $=\frac{1}{2}(m-1)$ ist. Daraus folgt, dafs zunächst alle die $\nu_{\frac{1}{2}(m-1)}$ Quotienten $\mu=0, 1, 2, 3, \ldots \frac{1}{2}(m-3)$ *vorhanden* sein müssen, weil kein Quotient μ gröfser ist als der *letzte* und sie gruppenweise regelmäfsig um 1 zunehmen: dann aber noch $\frac{1}{2}(n-1)-\nu_{\frac{1}{2}(m-1)}$ Quotienten $\mu=\frac{1}{2}(m-1)$; denn der *nächste* auf den $\nu_{\frac{1}{2}(m-1)}$ten folgende Quotient ist um 1 gröfser als dieser und der *letzte* $\mu_{\frac{1}{2}(n-1)}$ ist es nach (33.) ebenfalls.

D. Die Quotienten μ haben also zusammengenommen folgende Werthe:

34. $$\left\{\begin{array}{l} \text{die ersten } \nu_1 \text{ Quotienten } \mu \text{ sind } =0, \\ \text{die folgenden } \nu_2-\nu_1 \text{ Quotienten } \mu \text{ sind } =1, \\ \text{die folgenden } \nu_3-\nu_2 \text{ Quotienten } \mu \text{ sind } =2, \\ \text{die folgenden } \nu_4-\nu_3 \text{ Quotienten } \mu \text{ sind } =3, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \text{die vorletzten } \nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)} \text{ Quotienten } \mu \text{ sind } =\frac{1}{2}(m-3), \\ \text{die letzten } \frac{1}{2}(n-1)-\nu_{\frac{1}{2}(m-1)} \text{ Quotienten } \mu \text{ sind } =\frac{1}{2}(m-1). \end{array}\right.$$

Die *Summe* der Werthe *aller* Quotienten μ ist also

35. $$S\mu = 0.\nu_1+1(\nu_2-\nu_1)+2(\nu_3-\nu_2)+3(\nu_4-\nu_3)\ldots\ldots+\tfrac{1}{2}(m-3)(\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)})+\tfrac{1}{2}(m-1)(\tfrac{1}{2}(n-1)-\nu_{\frac{1}{2}(m-1)}),$$

und dieses giebt, wenn man wegläfst was sich aufhebt,

21 *

$$S\mu = -\nu_1-\nu_2-\nu_3\ldots\ldots-\nu_{\frac{1}{2}(m-3)}-\nu_{\frac{1}{2}(m-1)}+\tfrac{1}{4}(m-1)(n-1) \text{ oder}$$

36. $S\mu+S\nu = \frac{1}{4}(m-1)(n-1)$.

Dieses ist die Gleichung (8. 1.) des Lehrsatzes.

Zweiter Fall (9.), *wenn m ungerade und n gerade ist.*

E. Ganz wie in (*A.*) sind die ersten ν_1 Quotienten μ gleich Null; die folgenden $\nu_2-\nu_1$ Quotienten $\mu=1$; die weiter folgenden $\nu_3-\nu_2$ Quotienten $\mu=2$ etc., die vorletzten $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten $\mu=\frac{1}{2}(m-3)$.

F. Sodann aber ist hier für die *letzte* der Gleichungen (2.), nemlich für $\frac{1}{2}nm=\mu_{\frac{1}{2}n}n+r_{\frac{1}{2}n}$,

37. $\frac{1}{2}nm = \frac{1}{2}(m-1)n+\frac{1}{2}n$.

Hier ist $\frac{1}{2}n>0$ und $<n$. Auch ist $\frac{1}{2}n-n=-\frac{1}{2}n<0$ und $\frac{1}{2}n+n=\frac{3}{2}n>n$. Also ist $\frac{1}{2}n$ der Rest $r_{\frac{1}{2}n}$ und folglich auch $\frac{1}{2}(m-1)$ in (37.) der Quotient $\mu_{\frac{1}{2}n}$, so dafs also

38. $\mu_{\frac{1}{2}n}=\frac{1}{2}(m-1)$ und $r_{\frac{1}{2}n}=\frac{1}{2}n$

ist, wie es (9. 2.) behauptet.

G. Wiederum wie in (*C.*) folgt, dafs alle die $\nu_{\frac{1}{2}(m-1)}$ Quotienten $\mu= 0, 1, 2, 3, \ldots \frac{1}{2}(m-3)$ *vorhanden* sind; und dann noch $\frac{1}{2}n-\nu_{\frac{1}{2}(m-1)}$ um 1 gröfsere Quotienten $\mu=\frac{1}{2}(m-1)$.

H. Die Quotienten μ haben also zusammengenommen folgende Werthe:

39.
- die ersten ν_1 Quotienten μ sind $=0$,
- die folgenden $\nu_2-\nu_1$ Quotienten μ sind $=1$,
- die folgenden $\nu_3-\nu_2$ Quotienten μ sind $=2$,
- . . . .
- die vorletzten $\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)}$ Quotienten μ sind $=\frac{1}{2}(m-3)$,
- die letzten $\frac{1}{2}n-\nu_{\frac{1}{2}(m-1)}$ Quotienten μ sind $=\frac{1}{2}(m-1)$.

Ihre *Summe* beträgt folglich

40. $$S\mu=0.\nu_1+1.(\nu_2-\nu_1)+2(\nu_3-\nu_2)+3(\nu_4-\nu_3)\ldots\ldots+\tfrac{1}{2}(m-3)(\nu_{\frac{1}{2}(m-1)}-\nu_{\frac{1}{2}(m-3)})+\tfrac{1}{2}(m-1)(\tfrac{1}{2}n-\nu_{\frac{1}{2}(m-1)}),$$

und dieses giebt, wenn man wegläfst was sich aufhebt,

$$S\mu = -\nu_2-\nu_3-\nu_4\ldots\ldots-\nu_{\frac{1}{2}(m-3)}-\nu_{\frac{1}{2}(m-1)}+\tfrac{1}{4}(m-1)n \text{ oder}$$

41. $S\mu+S\nu = \frac{1}{4}(m-1)n$;

welches die Gleichung (9. 1.) des Lehrsatzes ist.

Dritter Fall (10.), *wenn m gerade und n ungerade ist.*

I. Ganz wie in (*A.*) sind die ersten ν_1 Quotienten μ gleich Null; die folgenden $\nu_2-\nu_1$ Quotienten μ sind $=1$, die weiter folgenden $\nu_3-\nu_2$ Quotienten

$\mu = 2$ etc. Die letzte Gleichung (3.) ist aber hier $\frac{1}{2}mn = \nu_{\frac{1}{2}m} m + \varrho_{\frac{1}{2}m}$, also steigt ν bis $\nu_{\frac{1}{2}m}$, und folglich sind die letzten Quotienten μ diejenigen $\nu_{\frac{1}{2}m} - \nu_{\frac{1}{2}m-1}$, und ihr Werth ist $= \frac{1}{2}m - 1$.

K. Sodann ist für die letzte der Gleichungen (2.), nemlich für $\frac{1}{2}(n-1)m = \mu_{\frac{1}{2}(n-1)} n + r_{\frac{1}{2}(n-1)}$,

$$42. \quad \tfrac{1}{2}(n-1)m = (\tfrac{1}{2}m - 1)n + n - \tfrac{1}{2}m.$$

Hier ist $n - \frac{1}{2}m > 0$, weil $n > m$ sein soll, und zugleich $n - \frac{1}{2}m < n$. Auch ist $n - \frac{1}{2}m - n = -\frac{1}{2}m < 0$ und $n - \frac{1}{2}m + n = 2n - \frac{1}{2}m > n$. Also ist $n - \frac{1}{2}m$ der Rest $r_{\frac{1}{2}(n-1)}$, und folglich auch, aus (42.), $\frac{1}{2}m - 1$ der Quotient $\mu_{\frac{1}{2}(n-1)}$, so dafs

$$43. \quad \mu_{\frac{1}{2}(n-1)} = \tfrac{1}{2}m - 1 \quad \text{und} \quad r_{\frac{1}{2}(n-1)} = n - \tfrac{1}{2}m$$

ist, wie es (10. 2.) behauptet.

L. Hieraus folgt, dafs es aufser den letzten $\nu_{\frac{1}{2}m} - \nu_{\frac{1}{2}(m-1)}$ Quotienten μ in (*I.*), deren Werth schon $\frac{1}{2}m - 1$ war, *keine* weiter giebt. Denn der Werth des *letzten* $\frac{1}{2}(n-1)$ten μ in (2.) ist nach (43.) auch nur $= \frac{1}{2}m - 1$. So folgt denn also auch, dafs hier $\nu_{\frac{1}{2}m}$ selbst $= \frac{1}{2}(n-1)$ sein mufs. In der That ist für die letzte Gleichung $\frac{1}{2}mn = \nu_{\frac{1}{2}m} m + \varrho_{\frac{1}{2}m}$ in (3.)

$$44. \quad \tfrac{1}{2}mn = \tfrac{1}{2}(n-1)m + \tfrac{1}{2}m.$$

Hier ist $\frac{1}{2}m > 0$ und $< m$, also ist $\frac{1}{2}m$ der Rest $\varrho_{\frac{1}{2}m}$ und folglich auch $\frac{1}{2}(n-1)$ der Quotient $\nu_{\frac{1}{2}m}$, so dafs also

$$45. \quad \nu_{\frac{1}{2}m} = \tfrac{1}{2}(n-1) \quad \text{und} \quad \varrho_{\frac{1}{2}m} = \tfrac{1}{2}m$$

ist, wie es (10. 2.) behauptet.

M. Es sind also in dem gegenwärtigen dritten Falle überhaupt nur die in (*I.*) verzeichneten Quotienten μ vorhanden, und $\nu_{\frac{1}{2}m}$ ist $= \frac{1}{2}(n-1)$. Die Quotienten haben also folgende Werthe:

46. {
die ersten ν_1 Quotienten μ sind $= 0$,
die folgenden $\nu_2 - \nu_1$ Quotienten μ sind $= 1$,
die folgenden $\nu_3 - \nu_2$ Quotienten μ sind $= 2$,
die folgenden $\nu_4 - \nu_3$ Quotienten μ sind $= 3$,
. . . .
die *letzten* $\nu_{\frac{1}{2}m} - \nu_{\frac{1}{2}m-1}$ *oder* $\frac{1}{2}(n-1) - \nu_{\frac{1}{2}m-1}$ Quotienten μ sind $= \frac{1}{2}m - 1$.

Ihre Summe beträgt demnach

$$47. \quad S\mu = 0\nu_1 + 1(\nu_2 - \nu_1) + 2(\nu_3 - \nu_2) \ldots + (\tfrac{1}{2}m - 2)(\nu_{\frac{1}{2}m-1} - \nu_{\frac{1}{2}m-2}) + (\tfrac{1}{2}m - 1)(\tfrac{1}{2}(n-1) - \nu_{\frac{1}{2}m-1}),$$

oder, wenn man wegläfst was sich aufhebt,

$$48. \quad S\mu = -\nu_1 - \nu_2 - \nu_3 \ldots \nu_{\frac{1}{2}m-2} - \nu_{\frac{1}{2}m-1} + (\tfrac{1}{2}m - 1) \cdot \tfrac{1}{2}(n-1).$$

Dieses ist, da $\nu_1+\nu_2+\nu_3\ldots.+\nu_{\frac{1}{2}m-1}=S\nu-\nu_{\frac{1}{2}m}$ (7.) $=S\nu-\frac{1}{2}(n-1)$ (45.) ist, so viel als

$$S\mu = -S\nu+\tfrac{1}{2}(n-1)+(\tfrac{1}{2}m-1)\tfrac{1}{2}(n-1) \text{ oder}$$

$$49.\quad S\mu+S\nu = \tfrac{1}{2}m(n-1);$$

und dieses ist die Gleichung (10. 1.) des Lehrsatzes.

Vierter Fall (11), *wenn m gerade und n gerade ist.* ***N.*** Ganz wie in (*A.*) sind die ersten ν Quotienten $\mu=0$, die folgenden $\nu_2-\nu_1$ Quotienten μ sind $=1$; die folgenden $\nu_3-\nu_2$ Quotienten μ sind $=2$, u. s. w. Die letzte Gleichung (3.) ist hier $\frac{1}{2}mn=\nu_{\frac{1}{2}m}m+\varrho_{\frac{1}{2}m}$, also steigt hier ν bis $\nu_{\frac{1}{2}m}$; die letzten Quotienten μ sind hier diejenigen $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ und ihr Werth ist $=\frac{1}{2}m-1$.

O. Diese Quotienten μ kommen auch wirklich alle vor, und keiner mehr: denn die letzte der Gleichungen (2.) ist hier $\frac{1}{2}nm=\mu_{\frac{1}{2}n}n+r_{\frac{1}{2}n}$. Aus derselben folgt, dafs $r_{\frac{1}{2}n}$ mit n *aufgehen* und folglich $=n$ sein mufs, da die r nicht 0 und nicht $>n$ sein sollen (4.). Mithin ist hier nothwendig

$$50.\quad \mu_{\frac{1}{2}n} = \tfrac{1}{2}m-1 \quad\text{und}\quad r_{\frac{1}{2}n} = n;$$

wie es (11. 2.) behauptet. Ähnlich folgt aus der letzten Gleichung (3.), welche $\frac{1}{2}mn=\nu_{\frac{1}{2}m}m+\varrho_{\frac{1}{2}m}$ ist, dafs $\varrho_{\frac{1}{2}m}$ mit m *aufgehen* und also $=0$ sein mufs, da die ϱ nicht gröfser als $m-1$ sein sollen (5.), so dafs also

$$51.\quad \nu_{\frac{1}{2}m} = \tfrac{1}{2}n \quad\text{und}\quad \varrho_{\frac{1}{2}m} = 0$$

sein mufs; gemäfs (11. 2.). Die $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ Quotienten in (*N.*), an Werth $\frac{1}{2}m-1$, sind also die *letzten* μ, denn es sind nur $\frac{1}{2}n$ Quotienten μ in (2.) vorhanden, und $\nu_{\frac{1}{2}m}$ ist $=\frac{1}{2}n$ (51.); desgleichen ist der Werth *des* letzten $\mu_{\frac{1}{2}n}$ oder *der* letzten μ $=\frac{1}{2}m-1$ (50.); wie es für die $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ letzten Quotienten sein soll.

P. Die Quotienten μ haben also in dem gegenwärtigen vierten Falle folgende Werthe:

52.
- die ersten ν_1 Quotienten μ sind $=0$,
- die folgenden $\nu_2-\nu_1$ Quotienten μ sind $=1$,
- die folgenden $\nu_3-\nu_2$ Quotienten μ sind $=2$,
- die folgenden $\nu_4-\nu_3$ Quotienten μ sind $=3$,
- . . . .
- die *letzten* $\nu_{\frac{1}{2}m}-\nu_{\frac{1}{2}m-1}$ *oder* $\frac{1}{2}n-\nu_{\frac{1}{2}m-1}$ Quotienten μ sind $=\frac{1}{2}m-1$.

Ihre *Summe* beträgt daher

$$53.\quad S\mu = 0.\nu_1+1(\nu_2-\nu_1)+2(\nu_3-\nu_2)\ldots.+(\tfrac{1}{2}m-2)(\nu_{\frac{1}{2}m-1}-\nu_{\frac{1}{2}m-2}) + (\tfrac{1}{2}m-1)(\tfrac{1}{2}n-\nu_{\frac{1}{2}m-1}),$$

oder, wenn man wegläſst was sich aufhebt,

$$54.\quad S\mu = -\nu_1-\nu_2-\nu_3 \dots\dots -\nu_{\frac{1}{2}m-2}-\nu_{\frac{1}{2}m-1}+(\tfrac{1}{2}m-1)\tfrac{1}{2}n.$$

Dieses ist, da $\nu_1+\nu_2+\nu_3\dots\dots+\nu_{\frac{1}{2}m-1} = S\nu-\nu_{\frac{1}{2}m}$ (7.) $= S\nu-\frac{1}{2}n$ (51.) ist, so viel als

$$S\mu = -S\nu+\tfrac{1}{2}n+(\tfrac{1}{2}m-1)\tfrac{1}{2}n \text{ oder}$$

$$55.\quad S\mu + S\nu = \tfrac{1}{4}mn;$$

und dieses ist die Gleichung (11. 1.) des Lehrsatzes.

Q. Anm. Der Beweis ist im Wesentlichen dem des einfacheren Falles im vorigen Paragraph nachgebildet. Es ist wieder die Summirung der Gleichungen (34. 39. 46. und 52.), durch welche er insbesondere seine Entwickelung erhält. Eigenthümlich sind übrigens die aus willkürlicher Zertheilung eines Ausdrucks wie (32. 37. u. 42.) hergenommenen Folgerungen.

§. 39.

Lehrsatz.

Es sei u *eine beliebige ungerade positive ganze Zahl, die also nach* (§. 28. 10.) *immer durch*

$$1.\quad u = 4n \pm 1$$

ausgedrückt werden kann, wo n *eine positive ganze Zahl bezeichnet. Eine andere, zu* u *theilerfremde beliebige positive ganze Zahl sei* v. *Man setze*

$$2.\quad \begin{cases} v = \mu_1 u + r_1, \\ 2v = \mu_2 u + r_2, \\ 3v = \mu_3 u + r_3, \\ 4v = \mu_4 u + r_4, \\ \dots\dots\dots\dots \\ \frac{1}{2}(u-1)v = \mu_{\frac{1}{2}(u-1)} u + r_{\frac{1}{2}(u-1)}; \end{cases}$$

unter der Bedingung, daſs die sämmtlichen $r > 0$ *und* $< u$ *sind, und bezeichne*

3. *die Anzahl der Reste* r *in* (2.), *welche* $> \frac{1}{2}u$ *sind, durch* x *und die Summe der sämmtlichen Quotienten* μ *in* (2.), *also*

$$4.\quad \mu_1+\mu_2+\mu_3+\mu_4 \dots\dots + \mu_{\frac{1}{2}(u-1)} \text{ durch } S\mu.$$

Alsdann ist

$$5.\quad \Big\{ x \text{ gerade oder ungerade, je nachdem es die Zahl } s = n(v-1)+S\mu \text{ ist.}$$

Ist auch v *ungerade, eben wie* u, *so ist*

6. x *gerade oder ungerade, je nachdem es* $S\mu$ *ist.*

Beispiel 1. Es sei

7. $u = 4n-1 = 11$, also $n = 3$, $\frac{1}{2}(u-1) = 5$, $v = 15$.

Alsdann giebt (2.)

$$8. \quad \begin{cases} v = 1u + 4, \\ 2v = 2u + 8, \\ 3v = 3u + 12, \\ 4v = 5u + 5, \\ 5v = 6u + 9; \end{cases}$$

also ist in (5.)

$$9. \quad s = 3.14 + 1 + 2 + 3 + 5 + 6 = 59.$$

Die 3 Reste 8, 12 und 9 sind $> \frac{1}{2}u (= 5\frac{1}{2})$, also ist

$$10. \quad x = 3,$$

und s und x sind, gemäfs (5.), beide *zugleich ungerade*.

Desgleichen sind gemäfs (6.) hier, wo auch v *ungerade* ist, $x = 3$ und $S\mu = 1 + 2 + 3 + 5 + 6 = 17$ *beide zugleich ungerade*.

Beispiel 2. Es sei

11. $u = 4n+1 = 13$, also $n = 3$, $\frac{1}{2}(u-1) = 6$; $v = 18$.

Alsdann giebt (2.)

$$12. \quad \begin{cases} v = 1u + 5, \\ 2v = 2u + 10, \\ 3v = 3u + 15, \\ 4v = 5u + 7, \\ 5v = 6u + 12, \\ 6v = 8u + 4; \end{cases}$$

also ist in (5.)

$$13. \quad s = 3.17 + 1 + 2 + 3 + 5 + 6 + 8 = 76.$$

Die 4 Reste 10, 15, 7 und 12 sind $> \frac{1}{2}u (= 6\frac{1}{2})$, also ist

$$14. \quad x = 4;$$

und s und x sind, gemäfs (5.), beide *zugleich gerade*

Beweis A. Es sei für ein beliebiges $s$fache von v:

$$15. \quad sv = \mu_s u + r_s,$$

welche Gleichung, wenn man darin $s = 1, 2, 3, \ldots. \frac{1}{2}(u-1)$ setzt, die Gleichungen (2.) giebt. Die Gleichung (15.), mit 2 multiplicirt, giebt

$$16. \quad 2sv = 2\mu_s u + 2r_s.$$

Setzt man nun in (16.) der Reihe nach $s = 1, 2, 3, \ldots. \frac{1}{2}(u-1)$ und in (15.) der Reihe nach $s = 2, 4, 6, 8, \ldots. u-1$, so erhält man folgende *zwiefachen* Ausdrücke von $2v, 4v, 6v, \ldots. (u-1)v$, nemlich:

$$17. \begin{cases} 2v = 2\mu_1 u + 2r_1 = \mu_2 u + r_2, \\ 4v = 2\mu_2 u + 2r_2 = \mu_4 u + r_4, \\ 6v = 2\mu_3 u + 2r_3 = \mu_6 u + r_6, \\ 8v = 2\mu_4 u + 2r_4 = \mu_8 u + r_8, \\ \dots\dots\dots\dots \\ (u-1)v = 2\mu_{\frac{1}{2}(u-1)} u + 2r_{\frac{1}{2}(u-1)} = \mu_{u-1} u + r_{u-1}. \end{cases}$$

In den ersten dieser Ausdrücke von $2v$, $4v$, $6v$, ... $(v-1)$ kommen alle die Reste r_1, r_2, r_3, ... $r_{\frac{1}{2}(u-1)}$ vor, die sich in (2.) finden, und der ***allgemeine*** Ausdruck der Gleichungen (17.) ist

$$18. \quad 2\varepsilon v = 2\mu_\varepsilon u + 2r_\varepsilon = \mu_{2\varepsilon} u + r_{2\varepsilon};$$

wo $\varepsilon = 1, 2, 3, \dots \frac{1}{2}(u-1)$ sein kann.

B. *a.* Ist in (18.) $r_\varepsilon < \frac{1}{2}u$, so ist $2r_\varepsilon < u$ und zugleich > 0. ***Eben das*** ist $r_{2\varepsilon}$, und es giebt nur einen positiven Rest >0 und $<u$ für ein bestimmtes ε; also ist nothwendig $r_{2\varepsilon} = 2r_\varepsilon$, und folglich auch

$$19. \quad 2\mu_\varepsilon = \mu_{2\varepsilon}, \text{ wenn } r_\varepsilon < \tfrac{1}{2}u.$$

b. Ist hingegen in (18.) $r_\varepsilon > \frac{1}{2}u$, so ist $2r_\varepsilon > u$; also müfste der Quotient $2\mu_\varepsilon$ um 1 ***gröfser*** genommen werden, wenn $2r_\varepsilon = r_{2\varepsilon}$ sein sollte. Mithin ist nothwendig

$$20. \quad 2\mu_\varepsilon = \mu_{2\varepsilon} - 1, \text{ wenn } r_\varepsilon > \tfrac{1}{2}u.$$

c. ***Gleich*** $\frac{1}{2}u$ kann r nicht sein, weil nach der Voraussetzung u ***ungerade*** sein soll. Es kommen also in (17.) ***nur*** Reste $r < \frac{1}{2}u$ oder $r > \frac{1}{2}u$ vor.

C. Nun kommen in (17.), wie schon bemerkt, ***alle*** die Reste r_1, r_2, r_3, ... $r_{\frac{1}{2}(u-1)}$ vor, und x derselben sind nach der Voraussetzung $> \frac{1}{2}u$: also ist in jeder von x ***Gleichungen*** (17.) nach (*B. b.*) der Quotient μ ***links*** um ***1 gröfser*** als der Quotient μ ***rechts;*** in den ***übrigen*** $\frac{1}{2}(u-1)-x$ Gleichungen dagegen sind nach (*B. a.*) die Quotienten μ links und rechts einander ***gleich.***

Nimmt man also links und rechts die ***Summe*** aller Quotienten μ, so ergiebt sich

$$21. \quad 2\mu_1 + 2\mu_2 + 2\mu_3 \dots + 2\mu_{\frac{1}{2}(u-1)} = \mu_2 + \mu_4 + \mu_6 \dots \mu_{u-1} - x,$$

oder, wenn man

$$22. \quad \mu_2 + \mu_4 + \mu_6 \dots + \mu_{u-1} \text{ durch } S_2\mu$$

bezeichnet,

$$23. \quad x = S_2\mu - 2S\mu \ (4.).$$

Aber $2S\mu$ ist *immer* eine *gerade* Zahl: also ist x *gerade* oder ungerade, je nachdem es $S_2\mu$ (22.) ist.

D. Man setze in (15.) $u-\varepsilon$ statt ε, so ergiebt sich

$$24.\quad (u-\varepsilon)v = \mu_{u-\varepsilon}u + r_{u-\varepsilon},$$

und wenn man (15.) zu (24.) addirt,

$$25.\quad \varepsilon v + (u-\varepsilon)v \quad\text{oder}\quad uv = (\mu_\varepsilon + \mu_{u-\varepsilon})u + r_\varepsilon + r_{u-\varepsilon}.$$

Daraus folgt, dafs $r_\varepsilon + r_{u-\varepsilon}$ mit u *aufgehen* mufs (§. 18.). Es sind aber r_ε und $r_{u-\varepsilon}$ beide >0 und $<u$, also ist $r_\varepsilon + r_{u-\varepsilon} > 0$ und $<2u$. Daher mufs nothwendig

$$26.\quad r_\varepsilon + r_{u-\varepsilon} = u$$

sein. Mithin ist in (25.)

$$27.\quad uv = (\mu_\varepsilon + \mu_{u-\varepsilon})u + u,$$

und folglich, mit u dividirt, $v = \mu_\varepsilon + \mu_{u-\varepsilon} + 1$ oder

$$28.\quad \mu_{u-\varepsilon} = v - 1 - \mu_\varepsilon.$$

E. Man setze nun in (28.) der Reihe nach $\varepsilon = 1, 3, 5, 7 \ldots\ldots 2n-1$, so ergiebt sich

$$29.\quad \begin{cases} \mu_{u-1} = v-1-\mu_1, \\ \mu_{u-3} = v-1-\mu_3, \\ \mu_{u-5} = v-1-\mu_5, \\ \ldots\ldots\ldots\ldots\ldots \\ \mu_{u-2n+1} = v-1-\mu_{2n-1}. \end{cases}$$

Die *Anzahl* dieser Gleichungen ist n; denn wäre nur 1 Gleichung vorhanden, so würde der Zeiger 1 von μ rechterhand durch $2.1-1=1$ ausgedrückt werden; wären 2 Gleichungen vorhanden, der Zeiger 3 von μ durch $2.2-1=3$; wären 3 Gleichungen vorhanden, der Zeiger 5 von μ durch $2.3-1=5$, u. s. w.: allgemein, wenn n Gleichungen vorhanden wären, der Zeiger von μ durch $2.n-1$; und das ist wirklich der Zeiger von μ. Die *Summe* der Gleichungen (29.) ist also

$$30.\quad \mu_{u-1}+\mu_{u-3}+\mu_{u-5}\ldots\ldots+\mu_{u-2n+1} = n(v-1)-(\mu_1+\mu_3+\mu_5\ldots\ldots+\mu_{2n-1}).$$

F. Der Ausdruck (22.) ist so viel als

$$31.\quad \left.\begin{aligned} S_2\mu &= \mu_2+\mu_4+\mu_6\ldots\ldots+\mu_{2n} \\ &+\mu_{u-1}+\mu_{u-3}+\mu_{u-5}\ldots\ldots\mu_{u-2n+1} \end{aligned}\right\}\ \text{für } u=4n+1 \text{ und}$$

$$32.\quad \left.\begin{aligned} S_2\mu &= \mu_2+\mu_4+\mu_6\ldots\ldots+\mu_{2n-2} \\ &+\mu_{u-1}+\mu_{u-3}+\mu_{u-5}\ldots\ldots+_{u-2n+1} \end{aligned}\right\}\ \text{für } u=4n-1;$$

denn

33. $\begin{cases} \text{für } u = 4n+1 \text{ ist } u-2n+1 = 2n+2, \text{ also folgt } \mu_{u-2n+1} = u_{2n+1} \\ \qquad \text{in (31.) unmittelbar auf } u_{2n}, \text{ und} \\ \text{für } u = 4n+1 \text{ ist } u-2n+1 = 2n, \text{ also folgt } \mu_{u-2n+1} = u_2 \\ \qquad \text{in (32.) unmittelbar auf } u_{2n-2}. \end{cases}$

Setzt man nun in (31. u. 32.) für die *untere* Zeile ihre Werthe aus (30.), so ergiebt sich

34. $S_2\mu = \mu_2+\mu_4+\mu_6 \ldots\ldots + \mu_{2n}+n(v-1)-(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1})$
für $u = 4n+1$ und

35. $S_2\mu = \mu_2+\mu_4+\mu_6 \ldots\ldots + \mu_{2n-2}+n(v-1)-(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1})$
für $u = 4n-1$.

G. Addirt man in (34. u. 35.) auf beiden Seiten noch

$$2(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1}),$$

so ergiebt sich

36. $$S_2\mu+2(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1}) = \mu_2+\mu_4+\mu_6 \ldots\ldots + \mu_{2n}+n(v-1) + \mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1}$$
$$= \mu_1+\mu_2+\mu_3+\mu_4 \ldots\ldots + \mu_{2n}+n(v-1)$$
für $u = 4n+1$ und

37. $$S_2\mu+2(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1}) = \mu_2+\mu_4+\mu_6 \ldots\ldots + \mu_{2n-2}+n(v-1) + \mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-3}+\mu_{2n-1}$$
$$= \mu_1+\mu_2+\mu_3+\mu_4 \ldots\ldots + \mu_{2n-1}+n(v-1)$$
für $u = 4n-1$.

Es ist aber in (36.) das letzte μ_{2n} rechts $=\mu_{\frac{1}{2}(u-1)}$, da $2n = \frac{1}{2}(u-1)$ ist für $u=4n+1$, und in (37.) ist das letzte u_{2v-1} rechts *ebenfalls* $= \mu_{\frac{1}{2}(u-1)}$, da $2n-1 = \frac{1}{2}(u-1)$ ist für $u=4n-1$. Also geben (36. u. 37.) gleichmäfsig *Dasselbe*, nemlich

$$S_2\mu+2(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1}) = \mu_1+\mu_2+\mu_3+\mu_4 \ldots\ldots + \mu_{\frac{1}{2}(u-1)}+n(v-1)$$

oder

38. $$S_2\mu+2(\mu_1+\mu_3+\mu_5 \ldots\ldots + u_{2n-1}) = S\mu+n(v-1) \quad (4.).$$

Die hier zu $S_2\mu$ links addirte Zahl $2(\mu_1+\mu_3+\mu_5 \ldots\ldots + \mu_{2n-1})$, welche sie auch sein mag, ist aber *immer gerade:* also ist $S_2\mu$ *gerade* oder *ungerade,* je nachdem es $S\mu+n(v-1)$ ist. Nun war x *gerade* oder *ungerade,* je nachdem es $S_2\mu$ ist (*C.*): also ist x *gerade* oder *ungerade,* je nachdem es $S\mu+n(v-1)$ ist.

Dieses ist was der Lehrsatz in (5.) behauptet.

H. Ist auch v *ungerade,* gleichwie u, so ist $v-1$ *gerade,* also auch $n(v-1)$ *gerade.* Also ist x *gerade* oder *ungerade,* je nachdem es blofs $S\mu$ ist; gemäfs (6.).

1. Anm. Der Beweis des Satzes entwickelt sich insbesondere aus den *zwiefachen* Ausdrücken (17.) der *geraden* Vielfachen $2v$, $4v$, $6v$, ... von v.

§. 40.

Lehrsatz.

Wenn p *eine beliebige Stammzahl ist, so bleibt, wenn man die* p—1te *Potenz jeder beliebigen positiven oder negativen Zahl* z, *die nicht mit* p *aufgeht, durch* p *dividirt, immer der Rest* +1: *das heifst, die Gleichung*

$$1.\quad z^{p-1} = \mathfrak{S}p+1$$

findet für jede Stammzahl p *und für jeden beliebigen positiven oder negativen Werth von* z *Statt, der nicht mit* p *aufgeht. Jedoch findet sie nicht nothwendig Statt, wenn* p *nicht eine Stammzahl ist, sondern Factoren* >1 *hat.*

Diesen Satz nennt man gewöhnlich, nach seinem Erfinder, den Fermatschen Satz.

Auch ist immer

$$2.\quad z^{p-1} = \mathfrak{S}(z^{\delta}-1)p+1,$$

wo δ *einen beliebigen Theiler von* p—1 *bezeichnet.*

Beispiele. 1. Es sei

$$3.\quad p = 13.$$

Ist hier z. B. $z = 11$, so ist $z^2 = 121 = \mathfrak{S}13+4$, $z^4 = \mathfrak{S}13+16 = \mathfrak{S}13+3$, $z^8 = \mathfrak{S}.13+9$, $z^{12} = z^{p-1} = z^4.z^8 = (\mathfrak{S}13+3)(\mathfrak{S}13+9) = \mathfrak{S}13+27 = \mathfrak{S}13+1$; gemäfs (1.).

Ist $z = 2$, so ist $z^3 = 8$, $z^6 = 64 = \mathfrak{S}p-1$, $z^{12} = z^{p-1} = \mathfrak{S}p+1$; ebenfalls gemäfs (1.); und so giebt *jedes* andere, nicht durch p theilbare z, $z^{p-1} = \mathfrak{S}p+1$. Ist $z > p$, so ist es so viel als $z = \mathfrak{S}p+z_1$, wo nun $z_1 < p$. Ist z *negativ*, so hat z^{p-1} gleichwohl denselben Rest $+1$, indem der Exponent $p-1$ von z für $p = 13$ und für jede andere *ungerade* Stammzahl *gerade* ist.

2. Es sei

$$4.\quad p = 2,$$

so ist $p-1 = 1$ und also $z^{p-1} = z$ selbst. Alle mit $p = 2$ nicht aufgehenden Zahlen, das heifst alle *ungeraden* positiven und negativen Zahlen lassen aber, durch 2 dividirt, offenbar den Rest $+1$. Z. B.: -15 ist gleich $-8.2+1$. Also auch für die einzige *gerade* Stammzahl $p = 2$ findet der Satz Statt.

Beweis *A*. Es kann immer

$$5.\quad mz = \mathfrak{G}p + r,$$

gesetzt werden, wo, wenn m eine *beliebige* ganze Zahl bedeutet,

$$6.\quad r \text{ eine der Zahlen } 1, 2, 3, 4, \ldots\ldots p-1$$

ist, aber nicht 0 sein kann, weil z nicht mit p aufgehen soll.

B. Giebt man nun dem beliebigen m der Reihe nach die Werthe $1, 2, 3, 4, \ldots\ldots p-1$, so durchläuft nach (§. 34. I.) auch r alle die Werthe $1, 2, 3, 4, \ldots\ldots p-1$, obwohl in verschiedener Ordnung. Es ergeben sich also die $p-1$ Gleichungen

$$7.\quad \begin{cases} 1z = \mathfrak{G}p + r_1, \\ 2z = \mathfrak{G}p + r_2, \\ 3z = \mathfrak{G}p + r_3, \\ \ldots\ldots\ldots\ldots \\ (p-1)z = \mathfrak{G}p + r_{p-1}; \end{cases}$$

wo die r nun nothwendig alle die Zahlen $1, 2, 3, 4 \ldots\ldots p-1$ sind.

C. Multiplicirt man diese $p-1$ Gleichungen in einander, so ergiebt sich

$$8.\quad 1.2.3.4\ldots\ldots(p-1).z^{p-1} = \mathfrak{G}p + r_1 r_2 r_3 r_4 \ldots\ldots r_{p-1},$$

und hieraus

$$9.\quad 1.2.3.4\ldots\ldots(p-1).z^{p-1} = \mathfrak{G}p + 1.2.3.4\ldots\ldots(p-1).$$

D. Aus (9.) folgt

$$10.\quad 1.2.3.4\ldots\ldots(p-1)(z^{p-1}-1) = \mathfrak{G}p.$$

Hier geht die Stammzahl p in *keinen* der Factoren $1, 2, 3, 4, \ldots\ldots p-1$ auf; denn alle sind $< p$. Also geht p auch in dem Producte $1.2.3.4\ldots\ldots p-1$ nicht auf (§. 22.). Da nun aber nach (8.) p nothwendig in die gesammte Gröfse $1.2.3.4\ldots\ldots(p-1)(z^{p-1}-1)$ aufgehen *mufs*, so mufs es in den noch übrigen Factor $z^{p-1}-1$ aufgehen (§. 25.) und also

$$11.\quad z^{p-1}-1 = \mathfrak{G}p$$

sein; woraus die Gleichung (1.) des Lehrsatzes folgt.

E. Alles Vorige bleibt dasselbe, wie grofs oder klein auch die Zahl z sein und ob sie positiv oder negativ sein mag, wenn sie nur nicht mit p aufgeht. Aber in diesem, und nur in diesem einzigen Falle von z findet das Bewiesene *nicht* Statt, indem dann r nicht eine der Zahlen (5.), sondern für *jedes* m gleich *Null* ist. Mithin gilt die Gleichung (1.) für jeden beliebigen positiven oder negativen ganzzahligen Werth von z, der *nicht* mit p aufgeht.

F. Ist p *nicht* eine *Stammzahl*, so findet zwar noch für jedes zu p *theilerfremde* z zufolge (§. 34.) Alles Statt, was oben (*A*., *B*., *C*.) behaupten,

denn auch dann noch sind die r nothwendig alle die Zahlen 1, 2, 3, 4, ... $p-1$ (§. 34. I.), aber aus der Gleichung (10.) folgt nun nicht mehr, dafs nothwendig $z^{p-1}-1$ mit p aufgehen mufs, weil schon einzelne Factoren von p in 1, 2, 3, 4 .... $p-1$ aufgehen können.

G. Nach (1.) ist $z^{p-1}-1=\mathfrak{G}p$. Aber $z^{p-1}-1$ geht für *jedes* z und $p-1$ mit $z^\delta-1$ auf, wenn δ in $p-1$ aufgeht, und giebt $z^{p-1-\delta}+z^{p-1-2\delta}+z^{p-1-3\delta}\ldots.+1$ zum Quotienten. Also mufs auch $\mathfrak{G}p$ mit $z^\delta-1$ aufgehen. Aber die Stammzahl p geht *nicht* mit $z^\delta-1$ auf, also mufs $\mathfrak{G}$ mit $z^\delta-1$ aufgehen und folglich

$$12.\quad z^{p-1}-1=\mathfrak{G}(z^\delta-1)p$$

sein; woraus die Gleichung (2.) folgt.

Anm. *H.* Der Beweis beruht insbesondere auf dem Umstande, dafs in (7.) die r nach (§. 34.) nothwendig alle die Zahlen 1, 2, 3, ... $p-1$ selbst sind.

Der *Fermat*sche Lehrsatz findet in der gesammten Theorie der Zahlen vielfache Anwendungen und ist also als einer der Hauptsätze derselben zu betrachten. Wie er sich ändert, wenn p *nicht* eine Stammzahl ist, wird weiter unten vorkommen

§. 41.

Lehrsatz.

Es sei p *eine beliebige Stammzahl* >2, z *eine beliebige ganze Zahl, die nicht mit* p *aufgeht.*

Man setze

$$1.\quad \begin{cases} z=\mathfrak{G}p+r_1, \\ 2z=\mathfrak{G}p+r_2, \\ 3z=\mathfrak{G}p+r_3, \\ 4z=\mathfrak{G}p+r_4, \\ \quad\cdots\cdots \\ \tfrac{1}{2}(p-1)z=\mathfrak{G}p+r_{\frac{1}{2}(p-1)}, \end{cases}$$

und bezeichne

2. *die Anzahl der Reste* r *in* (1.), *welche* $>\frac{1}{2}$p *sind, durch* z.

Alsdann ist

$$3.\quad z^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1, \text{ wenn } x \text{ gerade, und}$$

$$4.\quad z^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1, \text{ wenn } x \text{ ungerade ist.}$$

Das Eine und das Andere findet jedoch nothwendig nur dann Statt, wenn p *eine Stammzahl ist; nicht nothwendig, wenn* p *Theiler* >1 *hat.*

Beispiel 1. Es sei

$$5. \quad p = 13, \quad z = 20,$$

so giebt (1.)

$$6. \quad 1, 2, 3, 4, 5, 6.z = \mathfrak{S}p + 7, 1, 8, 2, 9 \text{ und } 3.$$

Die 3 Reste 7, 8 und 9 sind $> \frac{1}{2}p$, also ist $x = 3$ und *ungerade*. $z^{\frac{1}{2}(p-1)}$ ist $20^6 = \mathfrak{S}p + 7^6 = \mathfrak{S}p + 49^3 = \mathfrak{S}p - 3^3 = \mathfrak{S}p - 27 = \mathfrak{S}p - 1$; wie es nach (4.) sein soll.

Beispiel 2. Es sei

$$7. \quad p = 19, \quad z = 42,$$

so giebt (1.)

$$8. \quad 1, 2, 3, 4, 5, 6, 7, 8, 9.z = \mathfrak{S}p + 4, 8, 12, 16, 1, 5, 9, 13 \text{ und } 17.$$

Die 4 Reste 12, 16, 13 und 17 sind $> \frac{1}{2}p$, also ist $x = 4$ und *gerade*. $z^{\frac{1}{2}(p-1)}$ ist $42^9 = \mathfrak{S}p + 4^9 = \mathfrak{S}p + 64^3 = \mathfrak{S}p + 7^3 = \mathfrak{S}p + 343 = \mathfrak{S}p + 1$; gemäfs (4.).

Beweis. *A.* Man bezeichne diejenigen $\frac{1}{2}(p-1) - x$ Multiplicatoren von z in (1.), welche Reste $r < \frac{1}{2}p$ geben, durch m, die übrigen x Multiplicatoren, welche Reste $> \frac{1}{2}p$ geben, durch μ. Für die letzteren Vielfachen von z nehme man die Quotienten *um 1 gröfser*, also statt der *positiven* echten Reste r die *negativen echten* Reste, welche nun durch ϱ bezeichnet werden mögen, so dafs also die Gleichungen (1.) zusammen folgende sind:

$$9. \quad \begin{cases} m_1 z = \mathfrak{S}p + r_1, \\ m_2 z = \mathfrak{S}p + r_2, \\ m_3 z = \mathfrak{S}p + r_3, \\ \dots\dots\dots\dots \\ m_{\frac{1}{2}(p-1)-x} z = \mathfrak{S}p + r_{\frac{1}{2}(p-1)-x}; \end{cases} \qquad 10. \quad \begin{cases} \mu_1 z = \mathfrak{S}p - \varrho_1, \\ \mu_2 z = \mathfrak{S}p - \varrho_2, \\ \mu_3 z = \mathfrak{S}p - \varrho_3, \\ \dots\dots\dots \\ \mu_x z = \mathfrak{S}p - \varrho_x. \end{cases}$$

Alsdann sind zufolge (§. 35. 9.), da die Stammzahl p ungerade sein soll und zu jedem z theilerfremd ist, die r und ϱ in (9. u. 10.) zusammengenommen *alle die Zahlen*

$$11. \quad 1, 2, 3, 4, \dots \tfrac{1}{2}(p-1),$$

und x derselben sind *negativ*; während die m und μ *ebenfalls* alle die Zahlen (11.) sind.

B. Multiplicirt man also alle die $\frac{1}{2}(p-1)$ Gleichungen (9. u. 10.) in einander, so ergiebt sich

$$12. \quad 1.2.3.4 \dots \tfrac{1}{2}(p-1) z^{\frac{1}{2}(p-1)} = \mathfrak{S}p + 1.2.3.4 \dots \tfrac{1}{2}(p-1)(-1)^x,$$

und daraus folgt

$$13. \quad 1.2.3.4 \dots \tfrac{1}{2}(p-1)\left(z^{\frac{1}{2}(p-1)} - (-1)^x\right) = \mathfrak{S}p.$$

Zufolge dieser Gleichung mufs das Product linkerhand mit p aufgehen. Es geht aber keiner der Factoren $1, 2, 3, 4, \ldots \frac{1}{2}(p-1)$ des Productes mit p auf, weil alle $<p$ sind, also mufs der *letzte* Factor

$$14. \quad x^{\frac{1}{2}(p-1)} - (-1)^x = \mathfrak{G}p$$

sein (§. 25.), und daraus folgt

$$15. \quad x^{\frac{1}{2}(p-1)} = \mathfrak{G}p + (-1)^x;$$

welches für ein *gerades* x die Gleichung (3.) und für ein *ungerades* x die Gleichung (4.) des Lehrsatzes giebt.

C. Hätte p Factoren >1, so müfste wenigstens einer derselben $<\frac{1}{2}p$ sein, denn, alle $>\frac{1}{2}p$, würden eine Zahl $>p$ geben. Also geht dann in (13.) wenigstens ein Factor von p schon in $1.2.3.4 \ldots \frac{1}{2}(p-1)$ auf, und die Gleichung (14.) folgt nicht mehr aus (13.). Der Lehrsatz gilt also nur *nothwendig*, wenn p eine *Stammzahl* ist.

Anm. *D.* Der Beweis beruht insbesondere auf dem Satze (§. 35.).

§. 42.

Lehrsatz.

Es seien p *und* q *zwei beliebige Stammzahlen* >2, *die also immer durch*

$$1. \quad p = 4n \pm 1 \quad \text{und} \quad q = 4m \pm 1$$

ausgedrückt werden können (§. 28. IV.).

Man setze

$$2. \begin{cases} q = \mu_1 p + r_1, \\ 2q = \mu_2 p + r_2, \\ 3q = \mu_3 p + r_3, \\ \ldots\ldots\ldots\ldots \\ \frac{1}{2}(p-1)q = \mu_{\frac{1}{2}(p-1)} p + r_{\frac{1}{2}(p-1)}; \end{cases} \quad \text{und} \quad 3. \begin{cases} p = \nu_1 q + \varrho_1, \\ 2p = \nu_2 q + \varrho_2, \\ 3p = \nu_3 q + \varrho_3, \\ \ldots\ldots\ldots\ldots \\ \frac{1}{2}(q-1)p = \nu_{\frac{1}{2}(q-1)} q + r_{\frac{1}{2}(q-1)}; \end{cases}$$

und

$$4. \quad \mu_1 + \mu_2 + \mu_3 \ldots + \mu_{\frac{1}{2}(p-1)} = S\mu,$$

$$5. \quad \nu_1 + \nu_2 + \nu_3 \ldots + \nu_{\frac{1}{2}(q-1)} = S\nu.$$

Desgleichen bezeichne man

6. *die Anzahl der* $r > \frac{1}{2}p$ *in* (2.) *durch* k *und*

7. *die Anzahl der* $\varrho > \frac{1}{2}q$ *in* (3.) *durch* x.

Alsdann findet folgendes Gesetz Statt:

Erstlich. Sind nicht p *und* q *beide von der Form* $4n-1$ *oder* $4m-1$, *und ist also*

$$8.\quad \begin{cases} 1.\ \textit{entweder}\ \ p=4n+1, & q=4m+1, \\ 2.\ \textit{oder}\ \ p=4n+1, & q=4m-1, \\ 3.\ \textit{oder}\ \ p=4n-1, & q=4m+1, \end{cases}$$

so ist

9. 1. *zugleich* $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$ *und* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1$, *und zwar wenn* $S\mu$ *oder wenn* k *gerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *gerade ist;*
2. *zugleich* $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$ *und* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1$, *und zwar wenn* $S\mu$ *oder wenn* k *ungerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *ungerade ist.*

Zweitens. Sind p *und* q *beide von der Form* $4n-1$ *oder* $4m-1$, *und ist also*

$$10.\quad p=4n-1,\quad q=4m-1,$$

so ist

11. 1. *zugleich* $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$ *und* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1$, *und zwar wenn* $S\mu$ *oder wenn* k *gerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *ungerade ist;*
2. *zugleich* $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$ *und* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1$, *und zwar wenn* $S\mu$ *oder wenn* k *ungerade, worauf zugleich* $S\nu$ *oder* $\varkappa$ *gerade ist.*

Dieses Gesetz wird Reciprocitätsgesetz für Stammzahlen genannt. Auf Deutsch wird es also Gegenseitigkeitsgesetz für Stammzahlen heifsen müssen. Das Gesetz findet nur für Stammzahlen, nicht nothwendig für andere Zahlen Statt, welche Theiler >1 *mit einander gemein haben.*

Man bezeichnet auch,

12. *dafs z. B.* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q\pm1$ *sei, durch* $\left(\frac{p}{q}\right)=\pm1$.

Nach dieser Bezeichnung ist zufolge (9. u. 11.)

13. $\left(\frac{p}{q}\right)=+\left(\frac{q}{p}\right)$, *wenn* p *und* q *nicht beide von der Form* $4n-1$ *oder* $4m-1$ *sind, und*

14. $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$, *wenn* p *und* q *beide von der Form* $4n-1$ *oder* $4m-1$ *sind.*

Beispiel 1. Es sei

$$15.\quad p=13,\quad q=17,\quad \text{also}\ p=4n+1,\quad q=4m+1,$$

so ist in (2. u. 3.)

16.
$q=1p+4,\quad p=0q+13,$ also $S\mu=24,\quad q^1=\mathfrak{S}p+4,\quad p^1=\mathfrak{S}q+13,$
$2q=2p+8,\quad 2p=1q+9,\quad S\nu=24,\quad q^2=\mathfrak{S}p+3,\quad p^2=\mathfrak{S}q-1,$
$3q=3p+12,\quad 3p=2q+5,\quad k=4,\quad q^4=\mathfrak{S}p+9,\quad p^4=\mathfrak{S}q+1,$
$4q=5p+3,\quad 4p=3q+1,\quad \varkappa=4;\quad q^6=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p+27,\quad p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1.$
$5q=6p+7,\quad 5p=3q+14,\quad =\mathfrak{S}p+1;$
$6q=7p+11;\quad 6p=4q+10,$ Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$ und *zugleich* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1.$
$7p=5q+7,$ Desgleichen sind $S\mu$ und $S\nu$ und k und $\varkappa$ beide *gerade.*
$8p=6q+2$ Gemäfs (9. 1.).

Beispiel 2. Es sei

17. $p=13,\quad q=19,$ also $p=4n+1,\quad q=4m-1,$

so ist

18.
$q=1p+6,\quad p=0q+13,$ also $S\mu=27,\quad q^1=\mathfrak{S}p+6,\quad p^1=\mathfrak{S}q+13,$
$2q=2p+12,\quad 2p=1q+7,\quad S\nu=27,\quad q^2=\mathfrak{S}p+10,\quad p^2=\mathfrak{S}q-2,$
$3q=4p+5,\quad 3p=2q+1,\quad k=3,\quad q^4=\mathfrak{S}p+9,\quad p^4=\mathfrak{S}q+4,$
$4q=5p+11,\quad 4p=2q+14,\quad \varkappa=3;\quad q^6=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1;\quad p^8=\mathfrak{S}q-3,$
$5q=7p+4,\quad 5p=3q+8,\quad p^9=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1.$
$6q=8p+10;\quad 6p=4q+2,$ Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$ und *zugleich* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1.$
$7p=4q+15,$ Desgleichen sind $S\mu$ und $S\nu$ und k und $\varkappa$ beide *ungerade.*
$8p=5q+9,$ Gemäfs (9. 2.)
$9p=6q+3;$

Beispiel 3. Es sei

19. $p=11,\quad q=17,$ also $p=4n-1,\quad q=4m+1,$

so ist

20.
$q=1p+6,\quad p=0q+11,$ also $S\mu=21,\quad q^1=\mathfrak{S}p+6,\quad p^1=\mathfrak{S}q+11,$
$2q=3p+1,\quad 2p=1q+5,\quad S\nu=19,\quad q^2=\mathfrak{S}p+3,\quad p^2=\mathfrak{S}q+2,$
$3q=4p+7,\quad 3p=1q+16,\quad k=3,\quad q^4=\mathfrak{S}p+9,\quad p^4=\mathfrak{S}q+4,$
$4q=6p+2,\quad 4p=2q+10,\quad \varkappa=4,\quad q^5=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1;\quad p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1.$
$5q=7p+8;\quad 5p=3q+4,$ Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$ und *zugleich* $p^{\frac{1}{2}(q-1)}=\mathfrak{S}q-1.$
$6p=3q+15,$ Desgleichen sind $S\mu$ und $S\nu$ und k und $\varkappa$ beide *ungerade.*
$7p=4q+9,$ Gemäfs (9. 2.).
$8p=5q+3;$

Beispiel 4. Es sei

21. $p=7,\quad q=19,$ also $p=4n-1,\quad q=4m-1,$

so ist

$$22.\left\{\begin{array}{lllll}
q=2p+5, & p=0q+7, & \text{also } S\mu=15, & q^1=\mathfrak{S}p+5, & p^1=\mathfrak{S}q+7, \\
2q=5p+3, & 2p=0q+14, & S\nu=12, & q^2=\mathfrak{S}p+4, & p^2=\mathfrak{S}q+11, \\
3q=8p+1; & 3p=1q+2, & k=1, & q^3=q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1, & p^4=\mathfrak{S}q+7, \\
 & 4p=1q+9, & \varkappa=4; & & p^8=\mathfrak{S}q+11, \\
 & 5p=1q+16, & & & p^9=p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1. \\
 & 6p=2q+4, & \multicolumn{3}{l}{\text{Also ist } q^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1 \text{ und } \textit{zugleich } p^{\frac{1}{2}(q-1)}=\mathfrak{S}q+1.} \\
 & 7p=2q+11, & \multicolumn{3}{l}{\text{Desgleichen sind } S\mu \text{ und } k \textit{ ungerade} \text{ und } S\nu \text{ und } \varkappa \textit{ gerade}.} \\
 & 8p=2q+18, & \multicolumn{3}{l}{\text{Gemäfs (11. 2.)}} \\
 & 9p=3q+6; & & &
\end{array}\right.$$

Erster Beweis. *A.* Zufolge (§. 38. 8.) ist für zwei *beliebige ungerade* Zahlen m und n, also auch hier für die *ungeraden Stammzahlen* p und q,

$$23. \quad S\mu+S\nu = \tfrac{1}{4}(p-1)(q-1).$$

Dieses giebt für die 3 Fälle (*Erstlich.* 8.):

$$24.\left\{\begin{array}{ll}
1. & S\mu+S\nu = \tfrac{1}{4}(4n)(4m) = 4mn = \textit{einer geraden Zahl;} \\
2. & S\mu+S\nu = \tfrac{1}{4}(4n)(4m-2) = 2n(m-1) = \textit{einer geraden Zahl;} \\
3. & S\mu+S\nu = \tfrac{1}{4}(4n-2)(4m) = 2m(n-1) = \textit{einer geraden Zahl.}
\end{array}\right.$$

Also ist in den Fällen (*Erstlich.*) des Lehrsatzes $S\mu+S\nu$ *immer* eine *gerade* Zahl, und folglich sind $S\mu$ und $S\nu$ immer *zugleich* gerade oder *zugleich* ungerade; wie es in (9.) behauptet wird.

Für den Fall (*Zweitens.* 10.) dagegen giebt (23.)

$$25. \quad S\mu+S\nu = \tfrac{1}{4}(4n-2)(4m-2) = (2n-1)(2m-1)$$
$$= \text{einer } \textit{ungeraden} \text{ Zahl;}$$

also ist in dem Falle (*Zweitens.*) des Lehrsatzes $S\nu$ *gerade*, wenn $S\mu$ *ungerade* ist, und $S\nu$ *ungerade*, wenn $S\mu$ *gerade* ist.

B. Sodann ist nach (§. 39. 6.) in (2.) k gerade oder ungerade, je nachdem es $S\mu$ ist; denn so ist es zufolge (§. 39. 6.) für *beliebige ungerade* Zahlen u und v, also auch hier für die ungeraden Stammzahlen p und q. Nach (§. 41. 3. u. 4.) aber ist für eine beliebige Zahl z, die nicht mit p aufgeht, also auch hier für die Stammzahl q, $q^{\frac{1}{2}(p-1)} = \mathfrak{S}p \pm 1$, je nachdem k *gerade* oder *ungerade* ist. Also ist hier

$$26.\left\{\begin{array}{l}
q^{\frac{1}{2}(p-1)} = \mathfrak{S}p+1, \text{ wenn } S\mu \textit{ gerade} \text{ und} \\
q^{\frac{1}{2}(p-1)} = \mathfrak{S}p-1, \text{ wenn } S\mu \textit{ ungerade} \text{ ist.}
\end{array}\right.$$

So wird es in (9. u. 11.) behauptet.

C. Aber in den Fällen (*Erstlich.*) sind $S\mu$ und $S\nu$ *zugleich gerade* und *zugleich ungerade* (*A.*): also ist in diesen Fällen auch *zugleich*, weil

x und $S\nu$ eben so über $p^{\frac{1}{2}(q-1)}$, wie k und $S\mu$ über $q^{\frac{1}{2}(p-1)}$ entscheiden,

$$27. \quad \begin{cases} p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1, \text{ wenn } S\mu \text{ oder } S\nu \textit{ gerade}, \text{ und} \\ p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1, \text{ wenn } S\mu \text{ oder } S\nu \textit{ ungerade} \text{ ist.} \end{cases}$$

Dieses wird ferner in (9.) behauptet.

Dagegen ist in dem Falle (*Zweitens.*) $S\nu$ *ungerade*, wenn $S\mu$ *gerade* ist; und umgekehrt: also ist in diesem Falle

$$28. \quad \begin{cases} p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1, \text{ wenn } S\mu \textit{ gerade}, \text{ also } S\nu \textit{ ungerade} \text{ und} \\ p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1, \text{ wenn } S\mu \textit{ ungerade}, \text{ also } S\nu \textit{ gerade} \text{ ist.} \end{cases}$$

Dieses wird ferner in (11.) behauptet.

Zweiter Beweis. *D.* In (§. 36.) bezeichnet n_1 aus den mit v *aufgehenden* Zahlen $z < \frac{1}{2}uv$, also aus den Zahlen

$$29. \quad \begin{cases} v = \mathfrak{G}u+r_1, \\ 2v = \mathfrak{G}u+r_2, \\ 3v = \mathfrak{G}u+r_3, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \frac{1}{2}(u-1)v = \mathfrak{G}u+r_{\frac{1}{2}(u-1)}, \end{cases}$$

die Anzahl *derjenigen*, welche zu u Reste $r > \frac{1}{2}u$ lassen, und n_3, aus den mit u *aufgehenden* Zahlen $z < \frac{1}{2}uv$, also aus den Zahlen

$$30. \quad \begin{cases} u = \mathfrak{G}v+\varrho_1, \\ 2u = \mathfrak{G}v+\varrho_2, \\ 3u = \mathfrak{G}v+\varrho_3, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \frac{1}{2}(v-1)u = \mathfrak{G}v+\varrho_{\frac{1}{2}(v-1)}, \end{cases}$$

die Anzahl *derjenigen*, welche zu v Reste $\varrho > \frac{1}{2}v$ lassen.

Setzt man in (29. u. 30.) statt der dortigen, unter sich theilerfremden Zahlen u und v die gegenwärtigen, ebenfalls unter sich theilerfremden beiden Stammzahlen p und q, so sind die Gleichungen (29. u. 30.) diejenigen (2. u. 3.). Also ist für den gegenwärtigen Lehrsatz:

$$31. \quad n_1 = k \quad \text{und} \quad n_3 = x.$$

E. Nun ist zufolge (36. 16.)

$$32. \quad 2n_5 - n_1 - n_3 = \tfrac{1}{4}(u-1)(v-1),$$

also ist *hier*

$$33. \quad 2n_5 - (k+x) = \tfrac{1}{4}(p-1)(q-1).$$

Aber $\frac{1}{4}(p-1)(q-1)$ ist in den Fällen (*Erstlich.* 8.), wie aus (24.) erhellet, *immer gerade;* und nur in dem Falle (*Zweitens.* 10.) *ungerade.* Die Zahl $2n_5$, welche sie auch sein mag, ist *immer gerade,* also ist vermöge (33.)

34. $\begin{cases} k+x \text{ in den Fällen (\textit{Erstlich.} 8.) immer \textit{gerade}, und} \\ k+x \text{ nur in dem Falle (\textit{Zweitens.} 10.) \textit{ungerade};} \end{cases}$

woraus folgt, dafs

35. k und x in den Fällen (*Erstlich.* 8.) beide zugleich *gerade* oder *ungerade* sind und dafs
k und x in dem Falle (*Zweitens.* 10.), das eine *gerade*, das andere *ungerade* ist.

F. Zufolge (§. 41. 3. u. 4.) ist, da das dortige x für $z=q$ hier k und für $z=p$ und $p=q$ hier x ist,

36. $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, wenn k, und $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1$, wenn x *gerade* ist und

37. $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$, wenn k, und $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1$, wenn x *ungerade* ist;

also finden in den Fällen (*Erstlich.* 8.) vermöge (35.) die Gleichungen (36.) oder die Gleichungen (37.) *zugleich* Statt, und in dem Falle (*Zweitens.* 10.) findet die erste Gleichung (36.) mit der zweiten (37.), oder die zweite (36.) mit der ersten (37.) *zugleich* Statt; und zwar auf die Weise, wie es (9. u. 11.) aussagen.

G. Dafs $S\mu$ und k und $S\nu$ und x *zugleich gerade* oder *ungerade* sind, wie es (9. u. 11.) noch behaupten, folgt bei diesem zweiten Beweise aus (§. 39. 6.).

H. Dafs der Lehrsatz *nur* für Stammzahlen p und q, nicht nothwendig für andere Zahlen, welche Theiler >1 gemein haben, Statt findet, folgt daraus, dafs der Satz (§. 41.), auf welchem er mit beruht, *nur* für *Stammzahlen* nothwendig gilt.

Anm. *I.* Der erste Beweis beruft sich auf die Lehrsätze (§. 38. 39. und 41.), der zweite auf die Lehrsätze (§. 36., 39. und 41.); der erste also auf den Satz (§. 38.) von den *Quotienten* μ in den Gleichungen $((1, 2, 3, 4, \ldots \frac{1}{2}n \text{ oder } \frac{1}{2}(n-1))m = \mu n + r$, der zweite auf den Satz (§. 36.) von den *Resten* der Zahlen $1, 2, 3, 4, \ldots \frac{1}{2}(uv-1)$, dividirt durch u und v; aufserdem auf *dieselben* Sätze (§. 39. u. 41.). Die Sätze (§. 36. 38., 39. u. 41.) *bereiten* das Reciprocitäts- oder Gegenseitigkeitsgesetz für Stammzahlen *vor*. Sie sind aber von ihm getrennt und besonders aufgestellt worden, theils um den Beweis des gegenwärtigen Satzes an sich zu verkürzen und dadurch übersichtlicher zu machen, theils weil die vorbereitenden Sätze auch für sich selbst noch andere Anwendungen finden.

Das Reciprocitäts- oder Gegenseitigkeitsgesetz findet wieder in der gesammten Theorie der Zahlen vielfache weitere Anwendungen und ist daher, gleich dem *Fermat*sche Satze (§. 40.), ebenfalls als einer der Hauptsätze der Zahlenlehre zu betrachten. (Die Fortsetzung folgt.)

11.

Zusätze zu der Abhandlung über die Methode der kleinsten Quadrate, No. 22. im 26. Bd. d. J.

(Von Hrn. Dr. *Reuschle*, Prof. am Gymnasium zu Stuttgart.)

I. In §. 5. III. habe ich dem Functionenbeweise, wodurch *Encke* das arithmetische Mittel *a priori* darzuthun sucht, den Vorwurf gemacht, dafs er eben so gut auf jede andere symmetrische lineäre Function passe, wofern nicht eine neue Bedingung hinzutritt. Dafs eine solche in der bei *Encke* vorangestellten Forderung, für zwei Gröfsen müsse $x = \frac{1}{2}(a+b)$ sein, versteckt liege, ist mir vom Dr. *Zech* (dem Verfasser der interessanten Abhandlung über das Princip der kleinsten Wirkung im 24ten Bande dieses Journals) bemerklich gemacht worden. So wie allerdings der Werth von x bei zwei Gröfsen auf deren halbe Summe sich reduciren mufs, so kann in §. 5. III. nur $m = 1$ genommen, oder so kann nur mittels $s = a + b + c$ eliminirt werden; und das Wesen dieser Beweisführung besteht alsdann darin, dafs das arithmetische Mittel für jede Anzahl von Gröfsen nach analytischer Nothwendigkeit erwiesen wird, wenn es für zwei gilt: ein Fall, wo seine natürliche Plausibilität am stärksten hervortritt.

II. Von demselben talentvollen Mathematiker bin ich auf eine Schwierigkeit aufmerksam gemacht worden, die in der gebräuchlichen Bestimmung der Function φx aus dem Princip des arithmetischen Mittels steckt. Wenn nämlich der von *Gaufs* in der *Theoria motus* eingeschlagene Weg gegen sich hat, dafs die Functionalgleichung aus einer ganz speciellen, überdies als wirklich kaum denkbaren Voraussetzung über die Fehler hergeleitet wird, so drückt den Beweis im Jahrbuch, der keine besondere Voraussetzung macht, eine analytische Schwierigkeit.

Es seien $a, a', a'', \ldots.$ die beobachteten Werthe einer Gröfse, so ist ihr wahrscheinlichster Werth p, nach dem in §. 4. besprochenen Princip, derjenige, welcher die Function

$$P = \varphi x . \varphi x' . \varphi x'' \times \ldots.$$

zu einem Maximum macht; wobei nämlich

$$x = a - p, \quad x' = a' - p \text{ u. s. w.}$$

die Beobachtungsfehler sind; welcher also der Differentialgleichung

$$\frac{1}{\varphi x}\cdot\frac{d\varphi x}{dp}+\frac{1}{\varphi x'}\cdot\frac{d\varphi x'}{dp}+\ldots.=0$$

oder, wegen $\frac{d\varphi x}{dx}=-\frac{d\varphi x}{dp}$, der Gleichung

$$\Sigma\frac{1}{\varphi x}\cdot\frac{d\varphi x}{dx}=0$$

Genüge leistet, wofür wir endlich

$$\Sigma\psi x=0$$

schreiben, indem wir setzen:

$$\psi x=\frac{1}{\varphi x}\cdot\frac{d\varphi x}{dx}.$$

Aus dieser Gleichung ergiebt sich dann sogleich die endliche Beziehung

$$\varphi x=e^{\int dx.\psi x}$$

zwischen den Functionen φx und ψx, und es handelt sich um die Bestimmung der letztern. Nach den allgemeinen Bedingungen, an welche nach §. 3. die Function φx gebunden ist, mufs der Exponent von e eine gerade, mithin ψx eine ungerade Function von x sein, die mit x verschwindet und durchaus negative Coëfficienten hat, damit der Exponent von e immer negativ sei; und hierdurch ist bereits $\psi x=-cx$ als einfachste Form von ψx angedeutet. Dafs dies nun die wirkliche und einzige Form von ψx sei, wenn p das arithmetische Mittel sein soll, ist zu beweisen und mufs eine Folge davon sein, dafs die Gleichungen

1. $\Sigma\psi x=0$,
2. $\Sigma x=0$ (d. h. die des arithmetischen Mittels)

coexistiren, d. h. einerlei Werth von p geben. *Encke* behauptet nun, nachdem er der ersteren die Form

$$\Sigma x\frac{\psi x}{x}=0$$

gegeben hat, dafs diese *offenbar* nur dann mit der zweiten übereinstimmen könne, wenn der Quotient $\frac{\psi x}{x}$ auf eine Constante sich reducire, d. h. er fordert, dafs die beiden Gleichungen *identisch* seien. Allein zwei Gleichungen können einerlei Werth einer in ihnen gemeinschaftlich enthaltenen Gröfse geben, oder sie können *coexistiren*, ohne *identisch* zu sein: die eine kann ein Factor der andern sein, und diese noch mehrere, reelle oder imaginäre Werthe der Unbekannten enthalten. Darin besteht die oben erwähnte Schwie-

rigkeit, und es wäre nun entweder die Unmöglichkeit des so eben angedeuteten Umstandes zu beweisen, was meinen Versuchen nach nicht so leicht sein dürfte: oder es wäre dem Beweise eine andere Wendung zu geben, und ich glaube, dafs derselbe durch folgende Betrachtungen eben so gründlich als einfach wird.

Einmal gaben die beiden Gleichungen bei zwei Beobachtungen durch Elimination von x' sogleich

$$\psi x = -\psi(-x);$$

womit zugleich ψx als ungerade Function characterisirt ist.

Zweitens. Wenn man den Werth

$$x = -(x' + x'' + \dots)$$

aus der Gleichung

$$\Sigma x = 0$$

in die andere Gleichung setzt, in der Form

$$\psi x = -(\psi x' + \psi x'' + \dots),$$

so erhält man, mit Rücksicht auf das vorige Resultat:

$$\psi(x' + x'' + \dots) = \psi x' + \psi x'' + \dots,$$

woraus sogleich, nach dem in §. 1, 8. der Abhandlung citirten Satze, erhellet, dafs die Function ψx Proportionalität bedeutet, mithin, da überdies ihr Integral negativ sein mufs,

$$\psi x = -cx$$

ist, wo nun die Constante c eine positive Zahl bedeutet und woraus $\varphi x = e^{-h^2 x^2}$ folgt, indem $\frac{1}{2}c = h^2$ gesetzt wird.

12.

Bemerkungen zu den elliptischen und Abelschen Transcendenten.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

Das unendliche Product

$$1. \quad \Pi\left(1-\frac{x}{\lambda}\right) = \begin{cases} P(0;x) \\ P(1;x) \end{cases},$$

welches zwei Ausdrücke repräsentirt, je nachdem man den Index λ alle geraden oder alle ungeraden Werthe durchlaufen läfst, und in welchem wir uns den Factor $1+\frac{x}{0}$ durch x ersetzt denken, hat für jeden reellen und imaginären Werth von x einen ganz bestimmten Werth von der Form $p+q\sqrt{-1}$, der sich leicht durch Exponentialfunctionen, oder, was im Grunde dasselbe ist, durch Kreisfunctionen darstellen läfst; und umgekehrt geben die beiden unendlichen Producte, von welchen wir sprechen, eine vollständige Definition der allgemeinen Sinus und Cosinus oder der einfach-periodischen Functionen.

Die elliptischen Transcendenten, diese merkwürdige Gattung von Functionen, welche die Geometer in der neueren Zeit so vielfach beschäftigt hat, sind nichts anders, als Verbindungen durch die *Division* aus den vier unendlichen *Doppelproducten*, welche sich aus dem Product

$$2. \quad \Pi\left(1-\frac{x}{\lambda+\lambda' A}\right)$$

ergeben, wenn man das Multiplicationszeichen Π über alle geraden oder alle ungeraden Werthe von λ und eben so über alle geraden oder alle ungeraden Werthe von λ' ausdehnt, während A eine gegebene Constante vorstellt. Bezeichnen wir der Anschaulichkeit halber diese vier Producte durch

$$3. \quad P(0,0;x), \quad P(1,0;x), \quad P(0,1;x), \quad P(1,1;x),$$

wo die 0 jedesmal einem geraden, die 1 einem ungeraden Index entsprechen soll, so sind die drei gewöhnlich vorkommenden elliptischen Functionen durch die drei folgenden Quotienten gegeben:

$$4. \quad \frac{P(0,0;x)}{P(0,1;x)}, \quad \frac{P(1,0;x)}{P(0,1;x)}, \quad \frac{P(1,1;x)}{P(0,1;x)},$$

welche die merkwürdige Eigenschaft besitzen, doppelt-periodisch zu sein.

Die Constante A darf nie einen reellen Werth erhalten; denn für einen reellen und irrationalen Werth von A würde man auf unendlich viele Arten die ganzen Zahlen λ und λ' so bestimmen können, dafs der Ausdruck

$$\lambda + \lambda' A$$

kleiner wird, als eine beliebige, noch so kleine gegebene Zahl; und für einen rationalen Werth von A würde man eine Zahl finden können, welcher dieser Ausdruck für unendlich viele ganze Werthe von λ und λ' gleich wird; in beiden Fällen kann also das unendliche Product nicht convergiren. Man pflegt gewöhnlich A rein imaginär, d. h. von der Form $q\sqrt{-1}$ anzunehmen, wo q reell ist; aber man mag der Constante A einen complexen Werth geben, welchen man will: immer wird das unendliche Doppelproduct (2.) für jeden Werth von x einen ganz bestimmten Werth annehmen.

Aus der Definition, welche so eben von den elliptischen Transcendenten gegeben wurde, und welche umfassender sein dürfte, als die gewöhnliche, lassen sich auf sehr einfachem Wege alle Eigenschaften dieser Functionen herleiten. In kurzen Worten will ich ein Bild von dem Wege entwerfen, welchen man zu dem Ende nehmen könnte.

Zunächst kann man die unendlichen Doppelproducte durch wirkliche Ausführung der Multiplication nach einem der beiden Indices mit Hülfe der bekannten Formeln für die Kreisfunctionen auf eine doppelte Weise in einfache unendliche Producte verwandeln, und man erhält auf diesem Wege die bekannten Entwicklungen der elliptischen Functionen in unendliche Producte (*Evolutio prima; Jacobi Fundamenta nova pag. 86*). Betrachtet man die gewonnenen Resultate näher, so sieht man, dafs sie aus den zwei neuen Functionen bestehen:

$$5.\quad \begin{cases} \varphi(z) = \left(z + \varepsilon\frac{1}{z}\right)(1+\varepsilon q^2 z^2)\left(1+\varepsilon q^2 \frac{1}{z^2}\right)(1+\varepsilon q^4 z^2)\left(1+\varepsilon q^4 \frac{1}{z^2}\right) \text{ in inf.,} \\ \psi(z) = (1+\varepsilon q z^2)\left(1+\varepsilon q \frac{1}{z^2}\right)(1+\varepsilon q^3 z^2)\left(1+\varepsilon q^3 \frac{1}{z^2}\right) \text{ in inf.,} \end{cases}$$

wo z eine neue Variable vorstellt, die als Exponentialfunction von x erscheint, q eine Constante, die von A abhängt, und $\varepsilon = \pm 1$ ist.

Durch blofse Substitution der Werthe kann man sich nun überzeugen, dafs die beiden Functionen φ und ψ den Gleichungen

$$6.\quad \varphi(z) = \varepsilon q z^2 \varphi(qz) \quad \text{und} \quad \psi(z) = \varepsilon q z^2 \psi(qz)$$

genügen, mit deren Hülfe sich sogleich die Entwicklung in Reihen ausführen läfst. Man setze

$$\varphi(z) = \sum_{n=-\infty}^{n=\infty} K_{2n+1}\, z^{2n+1}, \qquad \psi(z) = \sum_{n=-\infty}^{n=\infty} L_{2n}\, z^{2n};$$

so erhält man vermöge der Gleichungen (6.) die Coëfficientengleichungen

$$K_{2n+3} = \varepsilon q^{2n+2} K_{2n+1},$$

$$L_{2n+2} = \varepsilon q^{2n+1} L_{2n},$$

aus welchen folgt:

$$7. \left\{ \begin{aligned} \varphi(z) &= K_1 \sum_{n=-\infty}^{n=\infty} \varepsilon^n q^{n(n+1)} z^{2n+1}, \\ \psi(z) &= L_0 \sum_{n=-\infty}^{n=\infty} \varepsilon^n q^{n^2} z^{2n}. \end{aligned} \right. \qquad \left\{ \textit{Evolutio tertia; Fundamenta pag. 188.} \right\}$$

Es ist sehr merkwürdig, dafs jede Potenz von φ und ψ, ja selbst jede beliebige homogene Function der beiden Functionen φ und ψ in eine ganz ähnliche Reihe entwickelt werden kann, wenn sie nur nicht vom 0ten Grade ist. Es sei in der That F eine homogene Function vom $k$ten Grade. Vermöge der Gleichungen (6.) ist

$$F[\varphi(z), \psi(z)] = F[\varepsilon q z^2 \varphi(qz), \varepsilon q z^2 \psi(qz)],$$

und vermöge der Eigenschaften der homogenen Functionen,

$$F[\varepsilon q z^2 \varphi(qz), \; \varepsilon q z^2 \psi(qz)] = \varepsilon^k q^k z^{2k} F[\varphi(qz), \psi(qz)].$$

Setzt man demnach $F[\varphi(z), \psi(z)] = G(z)$, so hat man die Relation

$$8. \qquad G(z) = \varepsilon^k q^k z^{2k} G(qz),$$

welche als Fundamentalformel für die Entwicklung benutzt werden mufs. Durch eine specielle Anwendung des eben angedeuteten Princips gelangt man auch dahin, zu beweisen, dafs die Functionen φ und ψ einer Differenzialgleichung von der Form

$$9. \quad \left[\varphi \frac{\partial \psi}{\partial x} - \psi \frac{\partial \varphi}{\partial x}\right]^2 = p\varphi^4 + p'\varphi^3\psi + p''\varphi^2\psi^2 + p'''\varphi\psi^3 + p''''\psi^4$$

genügen, oder dafs der Quotient $y = \frac{\varphi}{\psi}$ der Differentialgleichung

$$10. \qquad \left(\frac{\partial y}{\partial x}\right)^2 = p y^4 + p' y^3 + p'' y^2 + p''' y + p''''$$

genugthut, wo p, p' etc. Constanten sind, die nur von A abhängen.

§. 2.

Der so eben mit flüchtigen Worten angedeutete Gang möchte sich besonders Denjenigen empfehlen, welche durch die sehr complicirten Betrachtungen der Integralrechnung, von denen man gewöhnlich bei der Theorie der

elliptischen Transcendenten auszugehen pflegt, von dem Studium der letzteren abgeschreckt werden. Diese Betrachtungen scheinen sich auch in der That weniger zum Ausgangspuncte für eine so wichtige Theorie zu eignen, und bezeichnen wohl nur mehr den historischen Weg, auf welchem die Resultate gefunden worden sind. Die gewöhnliche Definition, welche man, ganz gegen die Analogie bei den Exponentialfunctionen, von den elliptischen Functionen giebt, ist diejenige, dafs sie die umgekehrten Functionen der bekannten Integrale sind, bei welchen die ganze Function unter der Quadratwurzel bis auf den vierten Grad steigt. Aber da schon die deutliche Vorstellung eines solchen Integrals, dessen Differential plötzlich vom Reellen zum Imaginären übergeht, nicht eben leicht ist, so möchte es wohl dem Lernenden fast unmöglich scheinen, sich *a priori* einen klaren Begriff von der Umkehrung einer solchen Integralfunction zu bilden, zumal da hier die geometrische Anschauung gebricht, welche man wenigstens bei den Kreisfunctionen noch zu Hülfe rufen kann. Eine besondere Schwierigkeit bringt die Periodicität hinein. Gehen wir, um nur von einer einfachen Periode zu reden, für einen Augenblick auf die Kreisfunctionen zurück. Wollte man für diese z. B. den Sinus als diejenige Function y von x definiren, welche durch die Gleichung

$$\int_0 \frac{\partial y}{\sqrt{(1-y^2)}} = x$$

gegeben ist, so müfste man, in Übereinstimmung mit den bekannten Eigenschaften der Sinus, behaupten, dafs das Integral für jeden gegebenen Werth von y unendlich viele verschiedene Werthe annimmt, obwohl dies mit der gewöhnlichen Bedeutung, welche man einem solchen Integrale (z. B. für $y < 1$) unterlegt, im Widerspruche steht. Auf dieselbe Weise müfste man wegen der doppelten Periodicität von $\sin \operatorname{am} x$ behaupten, dafs das elliptische Integral

$$\int_0 \frac{\partial y}{\sqrt{(1-y^2)}\sqrt{(1-k^2y^2)}} = x$$

für jeden Werth von y sogar unendlich mal unendlich viele verschiedene Werthe annimmt.

Noch gröfsere Schwierigkeiten zeigen sich bei den Abelschen Integralen. Die umgekehrten Functionen dieser Integrale müssen eine drei- oder mehrfache Periodicität besitzen. Nun darf man aber nur ganz einfach und consequent auf Dasjenige fortbauen, was *Jacobi* im 13ten Bande des gegenwärtigen Journals (*De funct. duarum variab. quadr. per.*) über die dreifache Periodicität sagt, um zu der Überzeugung zu gelangen, dafs unter dieser Voraussetzung ein

Abelsches Integral mit ganz bestimmter unterer Grenze für irgend einen gegebenen Werth des Variabeln alle möglichen reellen und imaginären Werthe annehmen kann. Geben wir dies zu, so hört das Abelsche Integral überhaupt auf, eine Function seines Variabeln zu sein. Da dies nun ein Widerspruch ist, so kann doch nur folgen, dafs das Abelsche Integral entweder keinen analytischen Sinn hat, oder, dafs die Definition, die man von einem Integral im Allgemeinen giebt, und aus welcher wir alle diese Folgerungen ableiten, nicht genügend ist. Um diesem Übelstande zu begegnen, führt der berühmte Verfasser der *Fundamenta,* z. B. für die Abelschen Integrale erster Ordnung, zwei Integrale zugleich ein, indem er

$$1.\quad \int_0 \frac{\partial x}{\sqrt{X}} = \varphi(x),\quad \int_0 \frac{x\,\partial x}{\sqrt{X}} = \varphi_1(x)$$

setzt, wo X eine ganze Function von x vom 5ten oder 6ten Grade ist, und betrachtet dann x und y als Functionen der Verbindungen

$$2.\quad \begin{cases} u = \varphi(x) + \varphi(y), \\ v = \varphi_1(x) + \varphi_1(y), \end{cases}$$

so dafs man

$$3.\quad x = \lambda(u, v);\quad y = \lambda_1(u, v)$$

hat. Aber wenn wir einmal zugeben, dafs die Function $\varphi(x)$ für jeden Werth von x alle möglichen Werthe erhalten kann, so wird auch $\varphi(y)$ dieselbe Eigenschaft für jeden Werth von y besitzen: also wird um so mehr die Summe u für jeden gegebenen Werth von x und y alle möglichen Werthe annehmen können. Dasselbe gilt von v; man sieht daher nicht deutlich, wie auf diese Weise von einer Abhängigkeit zwischen u, v, x und y die Rede sein kann. Diesem Einwande liefse sich nur insofern begegnen, als man sagte: zu jedem der unendlich vielen Werthe von u gebe es nur einen einzigen zugehörigen Werth von v; aber man müfste erst nachweisen, was unter solchen zusammengehörigen Werthen eigentlich zu verstehen sei. Es ist jedenfalls ebenso interessant, als nothwendig, sich vollkommene Klarheit über die Principien eines so höchst wichtigen Gegenstandes zu verschaffen.

§. 3.

Die Analogie, welche man gewöhnlich verfolgt, indem man von den Exponentialgröfsen und elliptischen Transcendenten zu neuen Functionen fortzuschreiten sucht, bezieht sich auf die Form der Integrale, oder, wenn man will, auf die *Form der Differentialgleichungen,* denen die Functionen ge-

nügen. Suchen wir jetzt eine andere Art von Analogie auf, indem wir uns wieder zu den Betrachtungen in §. 1. wenden. Zufolge der Bemerkung, die dort über die einfachen und doppelten unendlichen Producte in Beziehung auf Kreis- und elliptische Functionen gemacht wurden, müssen wir als das Analogon, welches gleichsam um eine Stufe höher steht, die *Quotienten aus den Quotienten* von unendlichen *Tripelproducten* von der Form

$$\Pi\left(1-\frac{x}{\lambda+\lambda' A+\lambda'' A'}\right),$$

wo A, A' Constanten und λ, λ', λ'' Indices nach der gewöhnlichen Bedeutung dieses Wortes sind, annehmen.

Es seien, um zu allgemeineren Betrachtungen überzugehen,

$$1.\quad \lambda_1,\ \lambda_2,\ \lambda_3,\ \ldots\ \lambda_n$$

n Indices und

$$2.\quad A_2,\ A_3,\ A_4,\ \ldots\ A_n$$

$n-1$ Constanten. Man setze der Kürze wegen

$$3.\quad \lambda_1+\lambda_2 A_2+\lambda_3 A_3+\ldots+\lambda_n A_n = N$$

und betrachte unter dieser Voraussetzung das Product

$$4.\quad \Pi\left(1-\frac{x}{N}\right),$$

in welchem sich das Multiplicationszeichen auf die Werthe von λ_1, λ_2 etc. bezieht. In einem solchen Producte dürfen wir, sobald $n>2$ ist, *nicht* die Indices, unabhängig von einander, alle möglichen Werthe von $-\infty$ bis $+\infty$ durchlaufen lassen, weil das Product, wegen der unendlich vielen Werthe von N, deren analytischer Modul unter einer noch so klein gegebenen Grenze liegen würde, nicht convergiren könnte, und weil man aufserdem auf Functionen mit drei und mehrfacher Periodicität geführt werden würde. Dasselbe findet sogar schon statt, wenn $n=2$ für den speciellen Fall eines reellen Werthes der Constante ist. Den mehrfachen Producten würde also nicht mehr, wie den einfachen und doppelten, ein bestimmter analytischer Sinn zukommen, wenn man den Indices alle möglichen Werthe zuertheilen wollte. Nichts hindert jedoch an der Betrachtung dieser mehrfachen Producte, sobald man die Indices gewissen *Beschränkungen* unterwirft, von der Beschaffenheit, dafs sie diejenigen Umstände beseitigen, welche die Nichtconvergenz herbeiführen: nemlich gewissen *Ungleichheitsbedingungen*, die man zwischen den Indices λ_1, λ_2, ... λ_n annehmen und dem Producte hinzufügen mufs, dergestalt, dafs das Multiplicationszeichen sich dann nur auf diejenigen Werthe derselben beziehend

gedacht wird, welche diesen Bedingungen genügen, während die übrigen ausgeschlossen bleiben. Ganz im Allgemeinen läfst sich hier über die Wahl dieser Bedingungsgleichungen nichts Näheres sagen. Aber es existirt eine ganze Classe solcher Functionen, welche in sehr enger Beziehung zu gewissen Resultaten der *Zahlentheorie* stehen; und gerade für diese besondere Gattung zeigen die Ungleichheitsbedingungen, von welchen wir reden, eine sehr eigenthümliche Beschaffenheit. Man findet nämlich für diese Fälle immer eine Verbindung aus einer bestimmten Anzahl von Werthen des Ausdrucks N, welche einen reellen und *ganzen* Werth annimmt; und die Ungleichheitsbedingungen kommen darauf hinaus, dafs sie eine ganze *Gruppe* unendlich vieler Werthe von N, für welche dieser Verbindung der nämliche Werth zukommt, und die als die Glieder geometrischer Reihen erscheinen, auf ein einziges N reduciren. Die Functionen, zu welchen man auf diesem Wege geführt wird, scheinen sehr merkwürdige Eigenschaften zu besitzen; sie eröffnen ein Feld, auf dem sich Stoff zu den reichhaltigsten Untersuchungen darbietet, und welches der eigentliche Grund und Boden zu sein scheint, auf welchem die schwierigsten Theile der Analysis und Zahlentheorie in einander greifen.

Übrigens lassen sich ganz ähnliche Betrachtungen, wie an die unendlichen Producte, auch an die *Reihen* knüpfen, zu welchen die Theorie der elliptischen Functionen führt.

Berlin am 10. Januar 1844.

13.

Note

extraite d'une lettre adressée à l'éditeur par Mr. *E. Catalan*, Répétiteur à l'école polytechnique de Paris.

„**Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le „théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à „le démontrer complètement: d'autres seront peut-être plus heureux:**

„**Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être „des puissances exactes; autrement dit: l'équation $x^m - y^n = 1$, dans „laquelle les inconnues sont entières et positives, n'admèt qu'une seule „solution.**"

Druckfehler im 24ten Bande.

Seite 171 Zeile 4 v. u. lies $\left(\frac{dfx}{dx}\right)_0 \Delta x$ statt $\left(\frac{dfx}{dr}\right)_0 \Delta x$
— — — — v. u. lies $\left(\frac{d^2fx}{dx^2}\right)_0 \frac{\Delta x^2}{2}$ statt $\left(\frac{d^2fx}{dx^2}\right) \frac{\Delta x^2}{2}$
— 175 — 2 v. u. l. s und S der zugehörige Bogen und Sector st. s der zugehörige Sector

Im 26ten Bande.

— 334 — 15 v. u. st. Linien-Ordinaten l. Linien, d. h. Ordinaten
— 336 — 11 v. u. st. n' l. n
— — — 12 v. u. st. $n i \varphi \alpha$ l. $n i \varphi x$
— 338 — 12 v. u. st. während l. indem
— 339 — 14 v. u. fehlt vor F das Zeichen $=$
— 344 — 14 v. u. st. Wahrscheinlichkeit l. Wahrscheinlichkeiten
— — — 6 v. u. st. Fehlergröfse, als Variabeln l. Fehlergröfse (als Variabeln)
— 345 — 7 v. o. st. α l. n
— — — 13 v. u. st. $F(x+h)$ l. $F(x+\Delta x)$
— 348 — 3 v. o. st. φx l. φx,
— 349 — 2 v. u. ist „wenig" auszustreichen.
— 350 — 10 v. u. st. $x = i\varphi x$ l. $w = i\varphi x$
— 351 — 3 v. u. ist „nebst dem" auszustreichen und dagegen in der nächsten Zeile statt „und constante" zu setzen: nebst constanten
— 354 — 11 v. u. ist nach combinirte ein , zu setzen.
— — — 10 v. u. st begriffenen zusammenfafste, l. zusammengefafst werden können,
— — — 6 v. u. st. Gröfse l. Gröfsen
— — — 5 v. u. st. die des l. das
— 355 — 1 v. o. st. die andere l. andere Formen
— — — 16 v. o. st. damit l. dafs
— — — 12 v. u. st. nähern l. unsern
— 359 — 16 v. o. ist „in" zu streichen.
— — — 8 v. u. fehlt: $\mu_m =$
— 362 — 2 v. o. st. wie r l. wie π
— — — 11 v. o. st. nemlich l. die Werthe:
— — — 17 v. o. st. die l. den

Im 27ten Bande.

— 76 — 25 en desc. au lieu de „seule formule que" lisez „seule que"
— 77 — 1 - - au lieu de α, β, γ lisez $\alpha, \beta, \gamma, \delta$
— 77 — 12 - - au lieu de „expression" lisez „l'expression"
— 87 — 2 v. o. st. *uneigentlich* l. *eigentlich*
— 87 — 4 v. o. st. *eigentlich* l. *uneigentlich*
— 87 — 15 v. o. st. $z^p = 1$ l. $z^{p-1} = 1$
— 87 — 21 v. o. st. Determinante l. regelmäfsige Determinante
— 88 — 18 v. o. st. $Y^2 + (-1)^{\frac{1}{4}(n-3)} Z^2$ l. $Y^2 + (-1)^{\frac{1}{4}(n-3)} . n Z^2$

Crelle, Journal d. Math. Bd. XXVII. Heft 2.

Facsimile einer Handschrift von Lexell.

Solutio Problematis Geometrici, in Actis Academiae Scientiarum Berolinensis pro Anno 177 a Celeb. Castillon propositi.

Auctore
A. J. Lexell.

1. Cum Illustris Eulerus de hoc Problemate sermonem iniiciens, dixisset se dubitare utrum ista solutio Analytica Illustris de la Grange, quam in Volumine Actorum Berolinensium citato, recensuit Celeb. Castillon, ad aliquam expeditam et concinnam constructionem Geometricam perducat; id quidem me incitavit ut disquirerem utrum ejusmodi constructio inde deduci possit, nec non et quum id quidem negotium mihi successerit, uti et constructionem pro alia solutione Analytica eliciendi; quae hac de re meditatus sum, nec non meditationes quasdam generales de hoc Problemate Geometrico non ingratas fore confido; etiamsi solutiones istae quas propositurus sum, elegantia et simplicitate multum concedant illis Geometricis constructionibus, quas Celeb. Mathematici Castillon, Eulerus et Fuss proposuerunt.

2. Dum igitur proponitur Problema: in circulo magnitudine positione et magnitudine dato inscribere triangulum

MCN

Cujus tria latera si opus sit producta per tria data puncta A, B, D transeant; solutio analytica sequenti ratione ad imitationem Illustr. de la Grange instituti patescit. Concipiantur a punctis datis A, B, D ad centrum circuli dati C ductae lineae rectae AC, BC, DC et ductis radiis circuli MC, NC, OC, ~~dicantur~~ exprimantur anguli ACM, ACN, ACO respective per x, y, z; anguli ACB, ACD per m, n, et lineae AC, BC, DC per a, b, c, tumque erit $BCO = z - m$; $BCN = y - m$, $DCM = n - x$, $DCO = n - z$. In triangulo igitur BCN habebimus ang. $CNB = 90 - \frac{1}{2}(BCN - BCO)$ et ang $CBN = 90 - \frac{1}{2}(BCN + BCO)$; hinc $\mathrm{Sin}\, CNB = \mathrm{Cos}\, \frac{1}{2}(y-z)$ et $\mathrm{Sin}\, CBN = \mathrm{Cos}(\frac{1}{2}(z+y) - m)$ Quum igitur sit:

$$BC : CN = \mathrm{Sin}\, CNB : \mathrm{Sin}\, CBN$$ obtinebimus inde

$$b : 1 = \mathrm{Cos}\, \tfrac{1}{2}(y-z) : \mathrm{Cos}(\tfrac{1}{2}(z+y) - m).$$

Simili prorsus ratiocinio pro triangulo DCM consequimur

$$c : 1 = \mathrm{Cos}\, \tfrac{1}{2}(z-x) : \mathrm{Cos}(\tfrac{1}{2}(z+x) - n).$$

Ex priori harum aequationum colligitur:

$$\mathrm{Cot}\, \tfrac{1}{2}z = \frac{b\, \mathrm{Sin}(\frac{1}{2}y - m) + \mathrm{Sin}\, \frac{1}{2}y}{\mathrm{Cos}\, \frac{1}{2}y - b\, \mathrm{Cos}(\frac{1}{2}y - m)}$$ et ex posteriori

$$\mathrm{Cot}\, \tfrac{1}{2}z = \frac{c\, \mathrm{Sin}(\frac{1}{2}x - n) + \mathrm{Sin}\, \frac{1}{2}x}{\mathrm{Cos}\, \frac{1}{2}x - c\, \mathrm{Cos}(\frac{1}{2}x - n)}$$; hi igitur valoribus inter se aequatis prodit ista analogia

$$b\, \mathrm{Sin}(\tfrac{1}{2}y - m) + \mathrm{Sin}\, \tfrac{1}{2}y : \mathrm{Cos}\, \tfrac{1}{2}y - b\, \mathrm{Cos}(\tfrac{1}{2}y - m) = c\, \mathrm{Sin}(\tfrac{1}{2}x - n) + \mathrm{Sin}\, \tfrac{1}{2}x :$$
$$\mathrm{Cos}\, \tfrac{1}{2}x - c\, \mathrm{Cos}(\tfrac{1}{2}x - n)$$, quae in lucem evolvitur si perficiant. etc.

14.

Transformations remarquables de quelques séries.

(Par Mr. G. *Eisenstein* à Berlin.)

J'ajoute aux formules présentées dans le premier cahier de ce volume *) l'équation suivante qui me parait surtout remarquable:

$$1. \quad \frac{\frac{1}{z}-\frac{1}{z^4}+\frac{1}{z^9}-\frac{1}{z^{16}}+\dots}{1-\frac{1}{z}+\frac{1}{z^4}-\frac{1}{z^9}+\dots} = \cfrac{1}{z-1+\cfrac{z}{z^3-1+\cfrac{z^3}{z^5-1+\cfrac{z^5}{z^7-1+\cfrac{z^7}{z^9-1+\text{etc.}}}}}}$$

De cette formule par un simple changement du signe de z résulte la suivante:

$$2. \quad \frac{\frac{1}{z}+\frac{1}{z^4}+\frac{1}{z^9}+\frac{1}{z^{16}}+\dots}{1+\frac{1}{z}+\frac{1}{z^4}+\frac{1}{z^9}+\dots} = \cfrac{1}{z+1-\cfrac{z}{z^3+1-\cfrac{z^3}{z^5+1-\cfrac{z^5}{z^7+1-\cfrac{z^7}{z^9+1-\text{etc.}}}}}}$$

Les lois de ces séries et des fractions continues sont manifestes.

Les séries et les fractions continues convergent ***rapidement,*** si l'on suppose, ce que nous faisons ici, que la variable z soit ***supérieure à l'unite.***

On voit que dans ce cas les dénominateurs des fractions continues sont toujours supérieurs aux numérateurs. En posant donc z égal à un nombre ***entier,*** on peut conclure, à l'aide d'un principe connu, que le rapport des deux séries qui composent le premier membre des équations (1.) et (2.) est un nombre ***irrationnel*** pour toute valeur entière de z. Nous tirons de là cette proposition remarquable:

---

*) Ces formules se trouvent à la fin d'une note ayant pour titre: „Théorèmes sur les formes cubiques etc."

Théorème. „*La lettre z désignant un entier quelconque positif ou négatif, mais supérieur à l'unité, la série*

$$1+\frac{1}{z}+\frac{1}{z^4}+\frac{1}{z^9}+\frac{1}{z^{16}}+\text{ in inf.}$$

aura toujours une valeur irrationnelle."

On peut tirer le même résultat de la première des formules que j'ai données à l'endroit cité plus haut, c'est à dire de la formule

$$3. \quad 1+\frac{x}{z}+\frac{x^2}{z^4}+\frac{x^3}{z^9}+\frac{x^4}{z^{16}}+\ldots = \cfrac{1}{1-\cfrac{x}{z-\cfrac{(1-z^2)x}{z^3-\cfrac{x}{z^3-\cfrac{(1-z^4)x}{z^4-\cfrac{x}{z^5-\text{etc.}}}}}}}$$

On peut tirer même de cette formule une conclusion encore beaucoup plus générale que la précédente. La voici:

Théorème. „*z désignant un entier quelconque, à l'exception de* ± 1, *et x étant une quantité rationnelle quelconque, inférieure ou tout au plus égale à l'unité, je dis que la somme de la série infinie*

$$1+\frac{x}{z}+\frac{x^2}{z^4}+\frac{x^3}{z^9}+\frac{x^4}{z^{16}}+\text{ etc.}$$

aura toujours une valeur irrationnelle.

Pour s'en assurer il suffit de supposer $x=\frac{m}{n}$, m et n étant deux entiers et $n>m$.

Par cette substitution la fraction continue prendra la forme

$$\frac{n}{m}\cdot\cfrac{m}{n-\cfrac{m}{z-\cfrac{(1-z^2)m}{nz^2-\cfrac{m}{z^3-\cfrac{(1-z^4)m}{nz^4-\cfrac{m}{z^5-\text{etc.},}}}}}}$$

où l'on voit que les dénominateurs finiront par surpasser toujours sans interruption les numérateurs.

Nous supprimons ici un grand nombre d'autres formules et de conséquences analogues.

Mr. ***Clausen*** a dit que ***la série celèbre de Lambert***

$$\frac{z}{1-z}+\frac{z^2}{1-z^2}+\frac{z^3}{1-z^3}+\frac{z^4}{1-z^4}+\text{etc.}$$

peut être transformée en celle-ci:

$$z\frac{1+z}{1-z}+z^4\frac{1+z^2}{1-z^2}+z^9\frac{1+z^3}{1-z^3}+z^{16}\frac{1+z^4}{1-z^4}+\text{etc.}:$$

proposition dont Mr. ***Scherk*** a donné une démonstration très simple *).

Je remarque que l'on peut aussi convertir la série de ***Lambert*** en quotient d'une autre série par un produit composé d'un nombre infini de facteurs, savoir de la manière suivante:

$$4.\quad \frac{z}{1-z}+\frac{z^2}{1-z^2}+\frac{z^3}{1-z^3}+\frac{z^4}{1-z^4}+\text{etc.}=$$

$$\frac{\frac{z}{1-z}-\frac{2z^3}{(1-z)(1-z^2)}+\frac{3z^6}{(1-z)(1-z^2)(1-z^3)}-\frac{4z^{10}}{(1-z)(1-z^2)(1-z^3)(1-z^4)}+\text{etc.}}{(1-z)(1-z^2)(1-z^3)(1-z^4)(1-z^5)\text{ in inf.}}.$$

Le produit infini $(1-z)(1-z^2)(1-z^3)(1-z^4)$ in inf. est le même dont ***Euler*** a donné une transformation si remarquable, en démontrant que ce produit est équivalent à la série suivante

$$1-z-z^2+z^5+z^7-z^{12}-\text{etc.}$$

qui a pour terme général

$$(-1)^n z^{\frac{1}{2}(3n^2\pm n)}.$$

Cette série peut encore être convertie en celle-ci:

$$5.\quad 1-\frac{z}{1-z}+\frac{z^3}{(1-z)(1-z^2)}-\frac{z^6}{(1-z)(1-z^2)(1-z^3)}+\text{etc.}$$

Peut-être fera-t'il plaisir à quelques lecteurs de voir ici le développement de la série de ***Lambert*** en fraction continue. Voici ce développement. On a

$$6.\quad \frac{z}{1-z}+\frac{z^2}{1-z^2}+\frac{z^3}{1-z^3}+\frac{z^4}{1-z^4}+\text{etc.}$$

$$=\cfrac{1}{t-1-\cfrac{(t-1)^2}{t^2-1-\cfrac{t(t-1)^2}{t^3-1-\cfrac{t(t^2-1)^2}{t^4-1-\cfrac{t^2(t^2-1)^2}{t^5-1-\cfrac{t^2(t^3-1)^2}{t^6-1-\cfrac{t^3(t^3-1)^2}{t^7-1-\text{etc.}}}}}}}}$$

où on a supposé pour plus de simplicité $t=\frac{1}{z}$.

---

*) Tome IX de ce journal.

La série de *Lambert* est convergente pour toutes les valeurs de z dont le module analytique est inférieur à l'unité, et elle est divergente pour toutes les valeurs de z dont le module est >1; on peut s'en convaincre facilement en considérant la limite du quotient de deux termes consécutifs

$$\frac{z^n}{1-z^n} : \frac{z^{n-1}}{1-z^{n-1}} = z . \frac{1-z^{n-1}}{1-z^n}$$

pour $n=\infty$. Mais pour une valeur de z dont le module est égal à l'unité, cette série se comporte bien singulièrement. En effet, en posant $z=e^{2\alpha\pi i}$, on peut dire que pour une valeur *rationnelle* de α la série aura une valeur infiniment grande, puisqu'elle renferme alors une infinité de termes de la forme $\frac{1}{0}$, mais que pour une valeur *irrationnelle* de α la valeur de la série sera indéterminée, de manière que la somme d'un nombre quelconque de termes sera toujours une expression assignable, mais qui ne convergera pas vers une limite fixe lorsqu'on y fait croître ce nombre au delà de toute limite.

J'ai donné à l'endroit cité le développement en fraction continue de la série finie

$$1+\varrho x+\varrho^4 x^2+\varrho^9 x^3+\dots+\varrho^{(m-1)^2} x^{m-1},$$

où ϱ désigne une racine primitive de l'équation

$$Z^m = 1,$$

m étant un nombre *impair*. Ce développement devient encore plus simple pour une valeur *paire* de l'exposant. Soit σ une racine primitive de l'équation

$$Z^{2m} = 1,$$

on aura

$$7. \quad 1+\sigma x+\sigma^4 x^2+\sigma^9 x^3+\dots+\sigma^{(2m-1)^2} x^{2m-1}$$

$$= \cfrac{1-x^{2m}}{1-\cfrac{x}{\sigma^{2m-1}-\cfrac{(1-\sigma^{2m-2})x}{\sigma^{2m-2}-\cfrac{x}{\sigma^{2m-3}-\cfrac{(1-\sigma^{2m-4})x}{\sigma^{2m-4}-\text{etc.} \; \ddots \; \cfrac{}{\sigma^3-\cfrac{(1-\sigma^2)x}{\sigma^2-\cfrac{x}{\sigma}}}}}}}}.$$

On peut prendre pour exemple $m=2$, ce qui donne l'équation

$$1+ix+x^2+ix^3 = \cfrac{1-x^4}{1-\cfrac{x}{-i-\cfrac{2x}{-1-\cfrac{x}{i}}}},$$

et se vérifie facilement par le calcul.

Par d'autres moyens je suis parvenu à une formule qui se rapporte aux formes *ternaires* (quadratiques), et qui me parait mériter quelque attention.

Soit

$$ax^2+a'x'^2+a''x''^2+2bx'x''+2b'xx''+2b''xx' = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} = f$$

une forme ternaire, où a, a', a'', b, b', b'' désignent des nombres entiers donnés, et x, x', x'' des indéterminées.

En posant

$$b^2-a'a''=A, \quad b'^2-aa''=A', \quad b''^2-aa'=A'',$$
$$ab-b'b''=B, \quad a'b'-bb''=B', \quad a''b''-bb'=B'',$$

il en résulte une autre forme ternaire

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} = F$$

que nous appelerons d'après Mr. *Gauss adjointe* à la forme f. En représentant de plus par D le nombre

$$D = ab^2+a'b'^2+a''b''^2-aa'a''-2bb'b'',$$

D sera le déterminant de la forme ternaire f. Cela posé, si la forme f est positive, c'est-à-dire si les nombres a, a', a'' sont positifs et A, A', A'', D négatifs, je dis qu'on aura entre la forme f et son adjointe F cette rélation de reciprocité remarquable:

$$8. \qquad m\sqrt{m}\,\Sigma\, e^{f.\frac{m\pi}{nD}} + nD\sqrt{n}\,\Sigma\, e^{F.\frac{n}{m}\pi} = 0,$$

où les séries sont triples et où les sommations indiquées par le signe Σ se rapportent à toutes les valeurs entières des indéterminées x, x', x'' renfermées dans les formes ternaires f et F. Quant à m et n, elle désignent deux quantités quelconques positives.

Il existe des rélations analogues pour les formes *quaternaires*, *quinaires* etc.

15.

Der Kreis-Umfang für den Durchmesser 1 auf 200 Decimalstellen berechnet

von Herrn *Z. Dahse* in Wien.

π = 3,14159 26535 89793 23846 26433 83279 50288 41971
69399 37510 58209 74944 59230 78164 06286 20899
86280 34825 34211 70679 82148 08651 32823 06647
09384 46095 50582 23172 53594 08128 4811|1 74502
84102 70193 85211 05559 64462 29489 54930 38196
2|6136|

Hiezu folgende Notiz aus einem Briefe des Herrn Prof. *von Schulz Strasznicky* zu Wien an den Herausgeber dieses Journals.

„Der bekannte Kopfrechner *Zacharias Dahse* aus Hamburg kam im J. 1840, nachdem er Nord-Deutschland durchreiset hatte, nach Wien, um öffentliche Proben seines erstaunlichen Rechentalents abzulegen. Der Ertrag hat ihm aber nicht einmal die dabei gehabten Auslagen gedeckt, und nur durch mehrere gütige Gönner, namentlich das hiesige Benedictiner Stift, „die Schottrer," wurde es ihm möglich, hier zu bleiben. Er besuchte meine Vorlesungen über Elementar-Mathematik am hiesigen k. k. polytechnischen Institute, und ich glaube ihn dahin gebracht zu haben, dafs er, unter der Leitung eines Mathematikers, mit seiner riesigen Rechenkraft der Wissenschaft nützliche Dienste leisten könne. Er hatte nun die Absicht, durch Süd-Deutschland und Frankreich nach England zu gehen. Da er sich mit den colossalsten, aber zwecklosen Rechnungen die Zeit vertrieb, forderte ich ihn zu einer Arbeit auf, die wenigstens ihm persönlich nützlich werden könne, und munterte ihn auf, die Ludolphische Zahl bis auf 200 Stellen zu berechnen. Unter den vorgeschlagenen Formeln wählte er sich

$$\tfrac{1}{4}\pi = \text{arc tang}\,\tfrac{1}{2} + \text{arc tang}\,\tfrac{1}{5} + \text{arc tang}\,\tfrac{1}{8},$$

und fand die obigen Ziffern.

Nach dieser Rechnung ergiebt sich, dafs von den 140 von *Vega* gerechneten Ziffern die letzten 4 unrichtig sind; was um so mehr daraus hervorgeht, da die Ziffern *Dase's* mit denen, die *Thibaut* in seinem Grundrifs der reinen Mathematik, 4te Aufl. 1822, S. 314 (wahrscheinlich nach dem Manuscript in der Rattcliffschen Bibliothek zu Oxford) angiebt, bis auf die letzten zwei Ziffern stimmen. Diese Übereinstimmung bürgt deshalb für die Richtigkeit der Rechnung, weil ich selbst erst nach Bekanntmachung der 200 Ziffern *Dase's* im hiesigen Zeitungsblatte auf die 156 Ziffern bei *Thibaut* aufmerksam gemacht wurde. Zu dieser Arbeit brauchte *Dase* kaum 2 Monate. Er will nun die Rechnung weiter treiben; allein ich habe ihn bereits vermocht, zu etwas Nützlicherem sich zu wenden. Meine Absicht mit der Berechnung der Ludolphischen Zahl durch *Dase* ging lediglich dahin, die gelehrte Welt Deutschlands auf ein Rechentalent aufmerksam zu machen, wie in Jahrhunderten kein zweites vorkommt; es war zunächst mein Wunsch, dafs der junge, brave, so selten talentvolle Mann Deutschland erhalten werde, und nicht bemüfsigt sei, in der Fremde ein wahrscheinlich kümmerliches Unterkommen zu suchen.

Unserm allverehrten Chef der Finanzen, dem Herrn Präsidenten Freiherrn von *Kübbek*, konnte eine so seltene Erscheinung nicht entgehen. Er stellte den jungen Mann bei der hiesigen Staats-Eisenbahn-Direction an, und der erleuchtete grofse Staatsmann erklärte ihm ausdrücklich, dafs dieses zunächst im Interesse der Wissenschaft geschehe; denn aufser 5 Stunden im Amt bleibt ihm die übrige Zeit des Tages frei.

Da so *Dase* einstweilen eine gesicherte Existenz hat, und von dem Wunsche glühet, sein aufserordentliches Talent dem Dienste der Wissenschaft zu widmen, so ist es nun unsere Aufgabe, diese so günstige Gelegenheit zu benutzen. *Dase* kann unter der Leitung eines Mathematikers für unser Tabellenwesen höchst Nützliches leisten. Zu was seine aufserordentlichen Kräfte zunächst zu benutzen seien, will ich dem Urtheil der Mathematiker Deutschlands unterwerfen. Meine Meinung wäre, durch ihn Tabellen für die elliptischen Functionen rechnen zu lassen; und wenn ich desfalls wagen dürfte, den gefeierten Herrn Professor *Jacobi* zu Königsberg um seine Anordnungen und Winke zu bitten, so würde ich es mir zur Ehre rechnen, sie hier mittels *Dase* in Vollzug zu setzen. Da ein edler Ehrgeiz den jungen Mann treibt, seinen Namen durch wissenschaftliche Dienste auf die Nachwelt zu bringen, so verlangt er kein Honorar für diese Arbeiten. Nur würden wir bitten, für den Verlag der so berechneten Tabellen zu sorgen, da hier für solche Sachen schwer ein Verleger zu finden wäre. *Dase* rechnet einstweilen ein Handbuch der natürlichen Logarithmen mit 7 Decimalen, ganz nach der Form der gewöhnlichen Logarithmen-Handbücher."

16.

Theoria novi multiplicatoris systemati aequationum differentialium vulgarium applicandi.

(Auctore *C. G. J. Jacobi*, prof. ord. math. Regiomonti.)

Argumentum.

§. 1.

Propositurus sum sequentibus *Euleriani* Multiplicatoris extensionem, per totum calculum integralem uberrimi usus et frequentissimae applicationis, eamque ab amplificationibus ab ipso *Eulero* et *Lagrange* factis diversissimam. Quae amplificatio maxime nititur analogia, quam in alia Commentatione pluribus prosecutus sum, inter quotientes differentiales et Determinantia functionalia. Efficit *Eulerianus* Multiplicator ut duae *duarum* variabilium functiones datae producant eiusdem functionis differentialia partialia. Respondent autem differentialibus partialibus Determinantia functionalia partialia, quae formari possunt quoties variabilium numerus numerum functionum superat, variis eligendo modis variabiles quarum respectu Determinans formetur Ita datis n functionibus $n+1$ variabilium earum functionum dabuntur $n+1$ Determinantia partialia; veluti si f et φ trium variabilium x, y, z functiones sunt, tria earum functionum Determinantia partialia erunt

$$\frac{\partial f}{\partial x}\cdot\frac{\partial \varphi}{\partial z}-\frac{\partial f}{\partial z}\cdot\frac{\partial \varphi}{\partial y},\quad \frac{\partial f}{\partial z}\cdot\frac{\partial \varphi}{\partial x}-\frac{\partial f}{\partial x}\cdot\frac{\partial \varphi}{\partial z},\quad \frac{\partial f}{\partial x}\cdot\frac{\partial \varphi}{\partial y}-\frac{\partial f}{\partial y}\cdot\frac{\partial \varphi}{\partial x}.$$

Quibus considerationibus motus, ut *Eulerianam* theoriam amplificarem, generaliter Multiplicatorem examinavi, in quem ducendae essent $n+1$ functiones $n+1$ variabilium ut producta haberi possent pro earundem n functionum Determinantibus functionalibus partialibus. Quemadmodum autem, proposita functione duarum variabilium, inter bina eius differentialia partialia intercedit aliqua conditio ex elementis nota, scilicet ut alterius differentiale secundum alteram variabilem sumtum alterius differentiali secundum alteram variabilem sumto aequale sit: ita inter illa $n+1$ Determinantia functionalia partialia inveni locum habere conditionem analogam. Singulis enim Determinantibus functionalibus partialibus respective secundum singulas variabiles differentiatis, aggregatum $n+1$ quantitatium provenientium videbimus identice evanescere. Quod suppe-

ditat aequationem differentialem partialem, cui Multiplicator ille satisfacere debeat, ei analogam qua *Eulerianus* Multiplicator definitur. Et vice versa, sicuti in theoria *Euleriana,* quamcunque quantitatem, aequationi illi differentiali partiali satisfacientem, videbimus pro Multiplicatore haberi posse. Unde ad Multiplicatorem aliquem obtinendum non necessarium erit ut illae n functiones ipsae innotescant.

Investigatio ipsius functionis duarum variabilium, cuius differentialia partialia datis functionibus proportionalia sint, pendet ab integratione completa aequationis differentialis vulgaris primi ordinis inter duas variabiles; quippe quae ea erit functio, quae Constanti Arbitrariae aequalis evadit. Multiplicator autem, qui functiones datas *aequales* efficit binis differentialibus eius functionis partialibus, ipsius *aequationis differentialis* Multiplicator appellatur. Qui aequationis differentialis integratione completa sponte suppeditatur, et vice versa eius cognitione ipsa integratio maxime expeditur, videlicet ad solas revocatur Quadraturas. Similiter datis $n+1$ variabilium $n+1$ functionibus, ut obtineantur n functiones quarum Determinantia partialia rationes easdem atque illae inter se habeant: facile patebit, integrandum esse systema n aequationum differentialium vulgarium primi ordinis, quo scilicet statuitur illarum $n+1$ variabilium differentialia esse in ratione ipsarum $n+1$ quantitatum propositarum. Quo complete integrato functiones, quae Constantibus Arbitrariis a se independentibus aequales evadunt, ipsae erunt n functiones quaesitae. Atque Multiplicatorem, qui $n+1$ quantitates datas Determinantibus earum functionum partialibus aequales efficit, per analogiam illius *systematis aequationum differentialium vulgarium Multiplicatorem* appello. Iam quidem complete integrato systemate aequationum differentialium vulgarium, eius facile innotescit Multiplicator; quippe ad quem inveniendum tantum opus est ut functionum Constantibus Arbitrariis aequalium, quae per integrationem completam constant, unum aliquod formetur Determinans partiale. At vice versa, cognito aliquo systematis aequationum differentialium Multiplicatore, sive quod idem est, cognita aliqua solutione aequationis differentialis partialis qua Multiplicator definitur, non ita patebat, utrum et quodnam inde commodum vel auxilium ad integrandum systema peti posset, ita ut nostri Multiplicatoris analogia cum *Euleriano* videretur in ea ipsa re deficere, qua propter olim *Eulerus* sui Multiplicatoris theoriam condidit. Contigit tandem usum introspicere plane singularem quem in integrando aequationum differentialium systemate e Multiplicatoris cognitione percipere liceat, quod scilicet eius ope non prima aliqua, sed omnium ultima integratio ad Quadraturas revocetur.

Hinc in theoria integrationis aequationum differentialium vulgarium novus disquisitionum aperitur campus, videlicet ultimas investigandi integrationes, dum primae non innotescunt. Quippe in vastis et luculentissimis problematis per theoriam hic propositam fit ut ultima generaliter absolvatur integratio, dum in casibus tantum particularibus Integralia prima invenire licet.

Capite primo examinabo Multiplicatoris nostri varias formas insigniores-que proprietates. In altero Capite eius monstrabo usum in integrando aequationum differentialium vulgarium systemate. In Capite tertio theoriam Multiplicatoris extendam ad systemata aequationum differentialium vulgarium cuiuslibet ordinis. In Commentationibus deinde subsequentibus mihi propositum est praecepta hic tradita variis illustrare applicationibus; e quibus est principium novum mechanicum latissime patens, nuper a me sine demonstratione divulgatum.

Caput primum.

Novi Multiplicatoris definitio et varii proprietates.

Lemma Fundamentale eiusque varii usus; de Determinantibus functionalibus partialibus.

§. 2.

Aequatione inter variabiles x et y proposita,

$$f(x, y) = \text{const.},$$

obtinetur differentialium dx et dy ratio,

$$dx : dy = \frac{\partial f}{\partial y} : -\frac{\partial f}{\partial x} \text{ *)}.$$

Si de hac ratione differentialium dx et dy sola agitur, in dextra parte aequationis antecedentis omittere licet differentialium partialium $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$ factorem vel denominatorem, si quo afficiuntur communem. Ubi vero pro quantitatibus, quae differentialibus dx et dy proportionales evadunt ipsa sumere placet $\frac{\partial f}{\partial y}$ et $-\frac{\partial f}{\partial x}$ vel $-\frac{\partial f}{\partial y}$ et $\frac{\partial f}{\partial x}$, qualia differentiatione partiali prodeunt, nullo

*) Differentialia vulgaria ut in aliis Commentationibus charactere — d —, partialia charactere — ∂ — denoto.

factore aut denominatore communi rejecto, eam conditionem formula analytica exprimi posse constat.

Videlicet si quantitas ipsi dx proportionalis differentiatur ipsius x respectu, quantitas ipsi dy proportionalis differentiatur ipsius y respectu, quantitatum differentiatione provenientium summa identice evanescere debet. Theorema simile ad plures variabiles valet.

Aequationibus enim inter x, y, z propositis,

$$f(x, y, z) = \text{Const.}, \quad \varphi(x, y, z) = \text{Const.},$$

obtinetur differentiando,

$$\frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy + \frac{\partial f}{\partial z} dz = 0,$$

$$\frac{\partial \varphi}{\partial x} dx + \frac{\partial \varphi}{\partial y} dy + \frac{\partial \varphi}{\partial z} dz = 0.$$

E quibus aequationibus eruuntur differentialium dx, dy, dz rationes,

$$dx : dy : dz = A : B : C,$$

siquidem ponitur

$$A = \frac{\partial f}{\partial y} \cdot \frac{\partial \varphi}{\partial z} - \frac{\partial f}{\partial z} \cdot \frac{\partial \varphi}{\partial y},$$

$$B = \frac{\partial f}{\partial z} \cdot \frac{\partial \varphi}{\partial x} - \frac{\partial f}{\partial x} \cdot \frac{\partial \varphi}{\partial z},$$

$$C = \frac{\partial f}{\partial x} \cdot \frac{\partial \varphi}{\partial y} - \frac{\partial f}{\partial y} \cdot \frac{\partial \varphi}{\partial x}.$$

Si tantum de rationibus differentialium dx, dy, dz agitur, factorem vel denominatorem communem quantitatum A, B, C, si quo afficiuntur, omittere licet. Ubi vero pro quantitatibus, quae differentialibus dx, dy, dz proportionales evadunt, ipsa sumere placet A, B, C, nullo factore vel denominatore communi rejecto, eam conditionem aliqua formula analytica exprimi posse videbimus. Fit enim

$$\frac{\partial A}{\partial x} = \frac{\partial \varphi}{\partial z} \cdot \frac{\partial^2 f}{\partial y \partial x} + \frac{\partial f}{\partial y} \cdot \frac{\partial^2 \varphi}{\partial z \partial x} - \frac{\partial \varphi}{\partial y} \cdot \frac{\partial^2 f}{\partial z \partial x} - \frac{\partial f}{\partial z} \cdot \frac{\partial^2 \varphi}{\partial y \partial x},$$

$$\frac{\partial B}{\partial y} = \frac{\partial \varphi}{\partial x} \cdot \frac{\partial^2 f}{\partial z \partial y} + \frac{\partial f}{\partial z} \cdot \frac{\partial^2 \varphi}{\partial x \partial y} - \frac{\partial \varphi}{\partial z} \cdot \frac{\partial^2 f}{\partial x \partial y} - \frac{\partial f}{\partial x} \cdot \frac{\partial^2 \varphi}{\partial z \partial y},$$

$$\frac{\partial C}{\partial z} = \frac{\partial \varphi}{\partial y} \cdot \frac{\partial^2 f}{\partial x \partial z} + \frac{\partial f}{\partial x} \cdot \frac{\partial^2 \varphi}{\partial y \partial z} - \frac{\partial \varphi}{\partial x} \cdot \frac{\partial^2 f}{\partial y \partial z} - \frac{\partial f}{\partial y} \cdot \frac{\partial^2 \varphi}{\partial x \partial z}.$$

Quae expressiones additae sese mutuo destruunt, unde eruitur,

$$\frac{\partial A}{\partial x} + \frac{\partial B}{\partial y} + \frac{\partial C}{\partial z} = 0,$$

hoc est, si quantitatem ipsi dx proportionalem ipsius x respectu, quantitatem

ipsi dy porportionalem ipsius y respectu, quantitatem ipsi dz proportionalem ipsius z respectu differentiamus, trium quantitatum differentiatione provenientium summa identice evanescere debet. Quae conditio prorsus analoga est ei, quae antecedentibus de duabus variabilibus tradita est atque e primis elementis constat. Antecedentia ad numerum variabilium quemcunque extendere licet, siquidem advocantur propositiones quas in *Diario Crell. Vol. XXIII.* de Determinantibus algebraicis et functionalibus tradidi et quarum per totam hanc Commentationem usum frequentissimum faciam. Habetur enim sequens

Lemma fundamentale.

„*Sint A, A_1, A_2, ... A_n quantites quae in Determinante Functionali*

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n}$$

respective per $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial x_1}$, $\frac{\partial f}{\partial x_2}$, ... $\frac{\partial f}{\partial x_n}$ *multiplicatae reprehenduntur, erit*

$$\frac{\partial A}{\partial x} + \frac{\partial A_1}{\partial x_1} + \frac{\partial A_2}{\partial x_2} \cdots + \frac{\partial A_n}{\partial x_n} = 0."$$

Demonstratio.

Secundum definitionem quantitatum A, A_1 etc. fit

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots + \frac{\partial f_n}{\partial x_n} = \frac{\partial f}{\partial x} A + \frac{\partial f}{\partial x_1} A_1 + \frac{\partial f}{\partial x_2} A_2 \cdots + \frac{\partial f}{\partial x_n} A_n.$$

Unde Lemma demonstratu propositum sic quoque exhibere licet:

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n} = \frac{\partial . fA}{\partial x} + \frac{\partial . fA_1}{\partial x_1} + \frac{\partial . fA_2}{\partial x_2} \cdots + \frac{\partial . fA_n}{\partial x_n}.$$

Facio hanc formulam iam demonstratam esse pro $n-1$ functionibus n variabilium, probabo Lemma ad n functiones $n+1$ variabilium valere.

Designo per (i, k) quantitatem quae in Determinante Functionali $\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdots \frac{\partial f_n}{\partial x_n}$ multiplicata reprehenditur per factorem

$$\frac{\partial f}{\partial x_i} \cdot \frac{\partial f_1}{\partial x_k}.$$

Constat autem per Determinantium proprietates iam olim ab ill. *Laplace* adnotatas, *bina Aggregata, in Determinante functionali proposito resp. per* $\frac{\partial f}{\partial x_i} \cdot \frac{\partial f_m}{\partial x_k}$ *et per* $\frac{\partial f}{\partial x_k} \cdot \frac{\partial f_m}{\partial x_i}$ *multiplicata, valoribus oppositis gaudere.* Unde sequitur

$$(i, k) = -(k, i) \quad \text{sive} \quad (i, k) + (k, i) = 0.$$

Est A_i complexus terminorum eius Determinantis qui per $\frac{\partial f}{\partial x_i}$ multiplicantur, unde fit

$$A_i = \frac{\partial f_1}{\partial x}(i, 0) + \frac{\partial f_1}{\partial x_1}(i, 1) + \frac{\partial f_1}{\partial x_2}(i, 2) \ldots + \frac{\partial f_1}{\partial x_n}(i, n),$$

qua in formula ipsum (i, i) aut omittendum aut $= 0$ ponendum est. Est porro A_i Determinans functionum $f_1, f_2, \ldots f_n$ formatum respectu variabilium $x, x_1, x_2, \ldots x_{i-1}, x_{i+1}, \ldots x_n$ atque sunt $(i, 0)$, $(i, 1)$ etc. quantitates quae in Determinante Functionali A_i multiplicatae reprehenduntur per $\frac{\partial f_1}{\partial x}$, $\frac{\partial f_1}{\partial x_1}$ etc. Unde si Lemma propositum ad $n-1$ functiones n variabilium valet, erit pro indicis i valoribus 0, 1, 2, ... n,

$$\frac{\partial (i, 0)}{\partial x} + \frac{\partial (i, 1)}{\partial x_1} \ldots + \frac{\partial (i, n)}{\partial x_n} = 0,$$

ideoque etiam

$$A_1 = \frac{\partial . f_1 (i, 0)}{\partial x} + \frac{\partial . f_1 (i, 1)}{\partial x_1} \ldots + \frac{\partial . f_1 (i, n)}{\partial x_n}.$$

Quae formula pro quolibet ipsius i valore 0, 1, 2, ... n valet. Iam generaliter observo, *quoties ponatur*

$$H_i = \frac{\partial . a_{i,0}}{\partial x} + \frac{\partial . a_{i,1}}{\partial x_1} \ldots + \frac{\partial . a_{i,n}}{\partial x_n},$$

designantibus $a_{i,k}$ ***quantitates quascunque pro quibus sit***

$$a_{i,k} + a_{k,i} = 0, \quad a_{i,i} = 0,$$

fieri

$$\frac{\partial H}{\partial x} + \frac{\partial H_1}{\partial x_1} + \frac{\partial H_2}{\partial x_2} \ldots + \frac{\partial H_n}{\partial x_n} = 0.$$

Bina enim differentialia inter se iuncta,

$$\frac{\partial . \frac{\partial . a_{i,k}}{\partial x_k}}{\partial x_i} + \frac{\partial . \frac{\partial . a_{k,i}}{\partial x_i}}{\partial x_k},$$

mutuo destruuntur, unde totam expressionem $\frac{\partial H}{\partial x} + \frac{\partial H_1}{\partial x_1} \ldots + \frac{\partial H_n}{\partial x_n}$ identice evanescere invenis. Ponendo autem $f_1 . (i, k) = a_{i,k}$, satisfit conditioni $a_{i,k} = -a_{k,i}$, porro fit $H_i = A_i$; ideoque

$$\frac{\partial A}{\partial x} + \frac{\partial A_1}{\partial x_1} \ldots + \frac{\partial A_n}{\partial x_n} = 0,$$

sive Lemma de n functionibus $n+1$ variabilium justum erit, dummodo de $n-1$ functionibus n variabilium locum habet. Unde tantum necesse est ut Lemma pro una functione duarum variabilium constet. Pro una autem functione f_1

duarum variabilium x et y abeunt quantitates A etc. in differentialia partialia $\frac{\partial f_1}{\partial y}$ et $-\frac{\partial f_1}{\partial x}$, ideoque Lemma redit in formulam

$$\frac{\partial . \frac{\partial f_1}{\partial x}}{\partial y} - \frac{\partial . \frac{\partial f_1}{\partial y}}{\partial x} = 0,$$

quae est differentialium partialium proprietas fundamentalis supra commemorata.

Lemma generale etiam directe demonstrari potest absque illa reductione numeri n ad numerum $n-1$. Nam cum A_i vacet differentialibus, ipsius x_i respectu sumtis, e quantitatibus $\frac{\partial A_i}{\partial x_i}$, nulla implicare potest differentialia bis secundum eandem variabilem sumta. Differentialia autem secunda, secundum variabiles diversas x_i et x_k sumta, non provenire possunt nisi e solis duobus terminis

$$\frac{\partial A_i}{\partial x_i} + \frac{\partial A_k}{\partial x_k}.$$

Unde ad probandum Lemma propositum sufficit ut demonstretur, in Aggregato $\frac{\partial A_i}{\partial x_i} + \frac{\partial A_k}{\partial x_k}$ se mutuo destruere terminos per quantitates $\frac{\partial^2 f_m}{\partial x_i \partial x_k}$ multiplicatos. Quod facile patet. Ponamus enim

$$A_i = \alpha_1 \frac{\partial f_1}{\partial x_k} + \alpha_2 \frac{\partial f_2}{\partial x_k} \dots + \alpha_n \frac{\partial f_n}{\partial x_k},$$

fit secundum Determinantium proprietatem, in priore demonstratione in usum vocatam,

$$A_k = -\left\{\alpha_1 \frac{\partial f_1}{\partial x_i} + \alpha_2 \frac{\partial f_2}{\partial x_i} \dots + \alpha_n \frac{\partial f_n}{\partial x_i}\right\}.$$

Quantitates α_1, α_2 etc. neque differentialibus secundum x_i sumtis, neque differentialibus secundum x_k sumtis afficiuntur. Unde substituendo ipsarum A_i et A_k expressiones antecedentes, de Aggregato

$$\frac{\partial A_i}{\partial x_i} + \frac{\partial A_k}{\partial x_k},$$

prorsus exulant differentialia secunda, secundum variabiles x_i et x_k sumta, terminis binis,

$$+\alpha_m \frac{\partial^2 f_m}{\partial x_k \partial x_i} - \alpha_m \frac{\partial^2 f_m}{\partial x_i \partial x_k},$$

se mutuo destruentibus. Erant autem inter omnes terminos Aggregati propositi

$$\frac{\partial A}{\partial x} + \frac{\partial A_1}{\partial x_1} + \frac{\partial A_2}{\partial x_2} \dots + \frac{\partial A_n}{\partial x_n}$$

soli termini $\frac{\partial A_i}{\partial x_i}+\frac{\partial A_k}{\partial x_k}$ qui affici possint differentialibus $\frac{\partial^2 f_m}{\partial x_i \partial x_k}$, unde in Aggregato proposito termini differentialibus secundis secundum x_i et x_k sumtis affecti se mutuo destruunt. Unde cum x_i et x_k binae quaecunque variabiles esse possint a se diversae, illud Aggregatum totum evanescit. Q. d. e.

Quoties numerus variabilium, quas datae functiones $f_1, f_2, \ldots f_n$ implicant, ipsum functionum numerum n superat, proponi potest, earum functionum Determinantia respectu quarumque n variabilium formare. Quae vocabo functionum $f_1, f_2, \ldots f_n$ *Determinantia Partialia* secundum analogiam denominationis de differentialibus usitatae.

Si numerus variabilium est $n+1$ sicuti antecedentibus, erit numerus Determinantium Functionalium Partialium $n+1$; si numerus variabilium est $n+2$, dabuntur $\frac{1}{2}(n+2)(n+1)$ Determinantia Functionalia Partialia, et ita porro. Eorum Determinantium Functionalium Partialium signa cum in arbitrio posita sint, casu quo variabilium numerus numerum functionum tantum unitate superat, supponam, signa omnium Determinantium ab eorum uno ita pendere, ut binorum Determinantium partialium alterum de altero deducatur, in signis differentialibus binarum variabilium independentium commutatione facta, omnium simul terminorum mutatis signis. Quem invenis esse habitum quantitatum $A, A_1, \ldots$ $\ldots A_n$, quae sunt functionum $f_1, f_2, \ldots f_n$ Determinantia partialia. Videlicet de uno

$$A = \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n},$$

deducitur $-A_i$, loco ipsorum

$$\frac{\partial f_1}{\partial x_i}, \quad \frac{\partial f_2}{\partial x_i}, \ldots \frac{\partial f_n}{\partial x_i}$$

respective scribendo

$$\frac{\partial f_1}{\partial x}, \quad \frac{\partial f_2}{\partial x}, \ldots \frac{\partial f_n}{\partial x}.$$

Pro una duarum variabilium x et y functione f_1 abibunt Determinantia partialia in differentialia partialia functionis f_1, alterum positivo alterum negativo signo sumtum,

$$\frac{\partial f_1}{\partial y}, \quad -\frac{\partial f_1}{\partial x} \quad \text{vel} \quad -\frac{\partial f_1}{\partial y}, \quad \frac{\partial f_1}{\partial x}.$$

Et quemadmodum inter differentialia partialia $\frac{\partial f_1}{\partial x}$ et $\frac{\partial f_1}{\partial y}$, locum habet formula fundamentalis,

$$\frac{\partial . \frac{\partial f_1}{\partial y}}{\partial x} - \frac{\partial . \frac{\partial f_1}{\partial x}}{\partial y} = 0,$$

ita $n+1$ variabilium $x, x_1, x_2, \ldots x_n$ propositis n functionibus $f_1, f_2, \ldots f_n$ Lemmate antecedente constituitur inter Determinantia Partialia $A, A_1, A_2, \ldots$ $\ldots A_n$ aequatio conditionalis fundamentalis,

$$\frac{\partial A}{\partial x}+\frac{\partial A_1}{\partial x_1}+\frac{\partial A_2}{\partial x_2}\ldots+\frac{\partial A_n}{\partial x_n}\doteq 0.$$

Quod igitur Lemma gravissimam manifestat analogiam Determinantium Functionalium et quotientium differentialium partialium.

Lemma traditum dedi olim in Commentatione, *Vol. VI. Diar. Crell. pg. 263 sqq. inserta, „De resolutione aequationum per series infinitas.“* Quod eo loco adhibui ad demonstrandam Propositionem quae et ipsa luculentam analogiam Determinantium Functionalium cum differentialibus constituit. Nam cum pateat seriei e solis variabilis x potestatibus conflatae quotientem differentialem vacare termino $\frac{1}{x}$, demonstravi, *serierum $f, f_1, \ldots f_n$, conflatarum e solis variabilium $x, x_1, \ldots x_n$ potestatibus, Determinans Functionale*

$$\Sigma\pm\frac{\partial f}{\partial x}\cdot\frac{\partial f_1}{\partial x_1}\cdot\frac{\partial f_2}{\partial x_2}\cdots\frac{\partial f_n}{\partial x_n}$$

vacare termino $\frac{1}{x x_1 x_2 \ldots x_n}$. Quippe Determinans antecedens per Lemma nostrum aequatur quantitati

$$\frac{\partial . fA}{\partial x}+\frac{\partial . fA_1}{\partial x_1}\ldots+\frac{\partial . fA_n}{\partial x_n},$$

cuius terminus primus evolutus vacare debet termino in $\frac{1}{x}$ ducto, secundus termino in $\frac{1}{x_1}$ ducto, et ita porro, ita ut in tota quantitate evoluta non obvenire possit terminus $\frac{1}{x x_1 x_2 \ldots x_n}$.

Quae propositio adhiberi potest ad amplificandum theoriam *Cauchyanam* residuorum dictam, eiusque ope radices systematis simultanei aequationum in series infinitas evolvi, quod in Commentatione citata videas.

Data occasione breviter adhuc innuam usum Lemmatis propositi in integralibus multiplicibus inter datos limites determinandis. Proponatur integrale multiplex,

$$\int U df\, df_1 \ldots df_n,$$

ponamusque limites, inter quos integratio afficienda sit, eo definiri, quod introducendo certas alias variabiles $x, x_1, \ldots x_n$ pro variabilibus independentibus, harum novarum variabilium limites a se invicem independentes sive constantes sint. Constat, novis variabilibus exhibitum integrale propositum fore,

$$\int U df\, df_1 \dots df_n = \int U \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \dots \frac{\partial f_n}{\partial x_n}\, dx\, dx_1 \dots dx_n.$$

Variabilibus propositis $f, f_1, \dots f_n$ expressa U integrataque ipsius f respectu, prodeat Π ita ut sit

$$\Pi = \int U \partial f, \quad U = \frac{\partial \Pi}{\partial f},$$

erit

$$U \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \dots \frac{\partial f_n}{\partial x_n} = \Sigma \pm \frac{\partial \Pi}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \dots \frac{\partial f_n}{\partial x_n}$$

Quod patet substituendo valores

$$\frac{\partial \Pi}{\partial x_i} = \frac{\partial \Pi}{\partial f} \cdot \frac{\partial f}{\partial x_i} + \frac{\partial \Pi}{\partial f_1} \cdot \frac{\partial f_1}{\partial x_i} \dots + \frac{\partial \Pi}{\partial f_n} \cdot \frac{\partial f_n}{\partial x_i},$$

et observando, post substitutionem factam evanescere quantitates omnes in

$$\frac{\partial \Pi}{\partial f_1}, \frac{\partial \Pi}{\partial f_2}, \dots \frac{\partial \Pi}{\partial f_n}$$

ductas. Fit autem e Lemmate proposito

$$\Sigma \pm \frac{\partial \Pi}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \dots \frac{\partial f_n}{\partial x_n} = \frac{\partial . \Pi A}{\partial x} + \frac{\partial . \Pi A_1}{\partial x_1} \dots + \frac{\partial . \Pi A_n}{\partial x_n}.$$

Unde eruitur formula reductionis

$$\int U df\, df_1 \dots df_n =$$

$$\int (\Pi A) dx_1 dx_2 \dots dx_n + \int (\Pi A_1) dx\, dx_2 \dots dx_n \dots + \int (\Pi A_n) dx\, dx_1 \dots dx_n.$$

Hic signo (ΠA_i) denoto, in functionibus $f, f_1, \dots f_n$ ipsi x substituendos esse binos eius limites constantes, binasque expressiones ipsius ΠA_i provenientes alteram de altera detrahendas esse. Hinc integrale $n+1$tuplex propositum videmus revocari ad $2n+2$ integralia $n$tuplicia. Quae singula eadem quidem formula exhiberi possunt

$$\int \Pi df_1 df_2 \dots df_n \; {}^{*}),$$

sed pro singulis erit Π diversa ipsarum $f_1, f_2, \dots f_n$ functio, limitesque ipsarum $f_1, f_2, \dots f_n$ diversi erunt. Singula deinde integralia $n$tuplicia eadem methodo ad $2n$ integralia $(n-1)$tuplicia revocari possunt, eaque ratione pergere licet, usque dum tota integratio inter limites propositos perfecta sit.

---

*) Habendo enim x pro Constante, fit

$$\int \Pi A dx_1 dx_2 \dots d_n = \int \Pi df_1 df_2 \dots df_n,$$

cum sit

$$A = \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \dots \frac{\partial f_n}{\partial x_n},$$

et similis formula pro reliquis integralibus valet.

Lemma traditum sub alia quoque forma proponi potest memoratu digna. Habeamus enim x, x_1, ... x_n pro ipsarum f, f_1, ... f_n functionibus, earumque quaeramus differentialia partialia, ipsius f respectu sumta. Quae per regulas notas inveniuntur,

$$\frac{\partial x}{\partial f} = \frac{A}{R}, \quad \frac{\partial x_1}{\partial f} = \frac{A_1}{R}, \quad \dots \quad \frac{\partial x_n}{\partial f} = \frac{A_n}{R},$$

siquidem R est Determinans propositum,

$$R = \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \dots \frac{\partial f_n}{\partial x_n}.$$

Hinc formula nostra

$$\frac{\partial A}{\partial x} + \frac{\partial A_1}{\partial x_1} \dots + \frac{\partial A_n}{\partial x_n} = 0,$$

si reputamus esse

$$\frac{\partial R}{\partial f} = \frac{\partial R}{\partial x} \cdot \frac{\partial x}{\partial f} + \frac{\partial R}{\partial x_1} \cdot \frac{\partial x_1}{\partial f} \dots + \frac{\partial R}{\partial x_n} \cdot \frac{\partial x_n}{\partial f},$$

formam induit sequentem,

$$0 = \frac{\partial R}{\partial f} + R \left\{ \frac{\partial . \frac{\partial x}{\partial f}}{\partial x} + \frac{\partial . \frac{\partial x_1}{\partial f}}{\partial x_1} \dots + \frac{\partial . \frac{\partial x_n}{\partial f}}{\partial x_n} \right\}$$

sive

$$0 = \frac{\partial \log R}{\partial f} + \frac{\partial . \frac{\partial x}{\partial f}}{\partial x} + \frac{\partial . \frac{\partial x_1}{\partial f}}{\partial x_1} \dots + \frac{\partial . \frac{\partial x_n}{\partial f}}{\partial x_n}.$$

In his formulis supponitur, ipsas R, x, x_1, ... x_n primum pro quantitatum f, f_1, ... f_n functionibus haberi omnesque secundum f differentiari; deinde differentialia partialia $\frac{\partial x}{\partial f}$, $\frac{\partial x_1}{\partial f}$ etc. rursus per ipsas x, x_1, ... x_n exprimi, et respective secundum x, x_1, ... x_n differentiari. Commutando quantitates x, x_1 etc. cum quantitatibus f, f_1 etc. formula antecedens in aliam abit, quam in *Diar. Crell.* Vol. XXII. pag. 336 demonstravi.

Novi Multiplicatoris definitio. Aequatio differentialis partialis cui satisfacit. Variae formae quas Multiplicatoris valor induere potest.

§. 3.

Sint X, X_1, ... X_n variabilium x, x_1, ... x_n functiones quaecunque non simul omnes identice evanescentes; proposita aequatione differentiali partiali lineari primi ordinis,

$$0 = X\frac{\partial f}{\partial x} + X_1 \frac{\partial f}{\partial x_1} \dots + X_n \frac{\partial f}{\partial x_n},$$

solutiones ejus exstant n a se invicem independentes. Quarum Determinantia partialia erunt inter se ut Coëfficientes aequationis differentialis partialis propositae $X, X_1, \ldots . X_n$. Solutionibus enim illis a se independentibus vocatis

$$f_1, f_2, \ldots . f_n,$$

habentur aequationes identicae,

$$0 = X\frac{\partial f_1}{\partial x} + X_1\frac{\partial f_1}{\partial x_1} \ldots . + X_n\frac{\partial f_1}{\partial f_n},$$

$$0 = X\frac{\partial f_2}{\partial x} + X_1\frac{\partial f_2}{\partial x_1} \ldots . + X_n\frac{\partial f_2}{\partial x_n},$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$0 = X\frac{\partial f_n}{\partial x} + X_1\frac{\partial f_n}{\partial x_1} \ldots . + X_n\frac{\partial f_n}{\partial x_n},$$

quae sunt n aequationes lineares inter $n+1$ quantitates $X, X_1, \ldots . X_n$, terminis carentes constantibus. Quibus aequationibus determinantur rationes quas ipsae X, X_1, etc. inter se tenent. Videlicet per regulas notas algebraicas invenitur, ipsas $X, X_1, \ldots . X_n$ esse inter se ut quantitates $A, A_1, \ldots . A_n$, §. pr. consideratas, quae erant complexus terminorum, in Determinante functionali

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \ldots . \frac{\partial f_n}{\partial x_n}$$

respective per $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial x_1}, \ldots . \frac{\partial f}{\partial x_n}$ multiplicatorum, sive functionum $f_1, f_2, \ldots$ $\ldots f_n$ Determinantia partialia. Sit M factor per quem Coëfficientes $X, X_1, \ldots X_n$ multiplicati ipsa producant Determinantia partialia $A, A_1, \ldots . A_n$, ita ut fiat:

$$1. \quad MX = A, \quad MX_1 = A_1, \quad \ldots . \quad MX_n = A_n.$$

Posito

$$R = \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \ldots . \frac{\partial f_n}{\partial x_n},$$

cum habeatur

$$R = A\frac{\partial f}{\partial x} + A_1\frac{\partial f}{\partial x_1} + \ldots . + A_n\frac{\partial f}{\partial x_n},$$

sequitur

$$2. \quad R = M\left(X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1} \ldots . + X_n\frac{\partial f}{\partial x_n}\right).$$

Iisdem substitutis formulis (1.) Lemma §. pr. demonstratum in hanc formulam abit:

$$3. \quad 0 = \frac{\partial . MX}{\partial x} + \frac{\partial . MX_1}{\partial x_1} \ldots . + \frac{\partial . MX_n}{\partial x_n}.$$

Habemus igitur Propositionem sequentem, qua Multiplicatoris M continetur definitio.

Propositio.

„Proponatur expressio

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n},$$

in qua sint X, X_1, ... X_n datae variabilium x, x_1, ... x_n functiones: functionibus f_1, f_2, ... f_n rite determinatis, ipsa f autem indeterminata manente, semper exstabit factor M, per quem multiplicata expressio proposita formam induat Determinantis functionalis

$$M\left(X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}\right)=\Sigma\pm\frac{\partial f}{\partial x}.\frac{\partial f_1}{\partial x_1}.\frac{\partial f_2}{\partial x_2}\dots\frac{\partial f_n}{\partial x_n},$$

isque Multiplicator satisfaciet aequationi differentiali partiali,

$$0=\frac{\partial.MX}{\partial x}+\frac{\partial.MX_1}{\partial x_1}\dots+\frac{\partial.MX_n}{\partial x_n}."$$

E valoribus ipsius M in sequentibus perpetuo excludo valorem $M=0$. Quem patet satisfacere aequationi (2.), qua Multiplicator definitur, dummodo statuatur functionum f_1, f_2, ... f_n unam reliquarum functionem esse; constat enim Determinans Functionale evanescere si functiones propositae non a se invicem sint independentes. Illo autem ipsius M valore excluso, Propositio antecedens inverti potest. Videlicet *si Multiplicator M definitur conditione ut pro functione indefinita f expressio,*

$$M\left(X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}\right)$$

evadat Determinans functionale,

$$R=\Sigma\pm\frac{\partial f}{\partial x}.\frac{\partial f}{\partial x_1}\dots\frac{\partial f_n}{\partial x_n},$$

functiones f_1, f_2, ... f_n necessario erunt solutiones a se independentes aequationis differentialis partialis linearis,

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}=0.$$

Nam pro ipsa f, quae erat functio indefinita, sumendo aliquam functionum f_1, f_2, ... f_n, identice evanescit Determinans R. Quod cum supponatur aequale expressioni,

$$M\left(X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}\right),$$

atque factor M a nihilo diversus statuatur, fieri debet ut substituendo ipsi f functiones f_1, f_2, ... f_n identice habeatur,

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}=0,$$

sive ut $f_1, f_2, \ldots. f_n$ ipsae sint aequationis differentialis partialis propositae solutiones. Eruntque solutiones illae $f_1, f_2, \ldots. f_n$ a se invicem independentes; si enim una reliquarum functio esset, Determinans R identice evanesceret pro functione f indefinita; unde etiam pro functione indefinita f evanescere deberet expressio

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\ldots.+X_n\frac{\partial f}{\partial x_n},$$

quod fieri non potest nisi omnes X, X_1 etc. simul identice evanescunt.

Datis functionibus $f_1, f_2, \ldots. f_n$ una quaelibet ex aequationum (1.) numero ad definiendum Multiplicatorem sufficit, veluti aequatio,

$$MX = A = \Sigma\pm\frac{\partial f_1}{\partial x_1}.\frac{\partial f_2}{\partial x_2}\ldots.\frac{\partial f_n}{\partial x_n},$$

e qua sequitur

$$4.\quad M = \frac{1}{X}\Sigma\pm\frac{\partial f_1}{\partial x_1}.\frac{\partial f_2}{\partial x_2}\ldots.\frac{\partial f_n}{\partial x_n}.$$

Qua tamen formula ut definiatur Multiplicator aequationis differentialis partialis propositae, addenda conditio est ut X et A non evanescant.

Pro duabus variabilibus x et x_1 Multiplicator antecedentibus definitus cum *Euleriano* convenit. Sint enim X, X_1 datae variabilium x et x_1 functiones, atque proponatur aequatio differentialis primi ordinis inter x et x_1,

$$Xdx_1-X_1dx = 0.$$

Est Multiplicator *Eulerianus* eiusmodi factor M per quem multiplicata pars laeva aequationis antecedentis abit in differentiale completum functionis alicuius f_1, ita ut sit

$$df_1 = \frac{\partial f_1}{\partial x}dx+\frac{\partial f_1}{\partial x_1}dx_1 = M(Xdx_1-X_1dx),$$

sive,

$$MX = \frac{\partial f_1}{\partial x_1},\qquad MX_1 = -\frac{\partial f_1}{\partial x}.$$

E quibus formulis sequitur, pro functione indefinita f induere expressionem,

$$M\left(X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\right),$$

formam Determinantis functionalis

$$\frac{\partial f}{\partial x}.\frac{\partial f_1}{\partial x_1}-\frac{\partial f}{\partial x_1}.\frac{\partial f_1}{\partial x},$$

et Multiplicatorem M satisfacere aequationi differentiali partiali,

$$\frac{\partial.MX}{\partial x}+\frac{\partial.MX_1}{\partial x_1} = 0.$$

Quae pro duobus variabilibus independentibus sunt eaedem proprietates characteristicae, quae Multiplicatori generali assignavi.

Problema solvendi aequationem differentialem partialem propositam,

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\,\ldots\,+X_n\frac{\partial f}{\partial x_n}=0,$$

cum duobus aliis problematis arctissime coniunctum est. Designante enim Π quamcunque aequationis praecedentis solutionem, ex aequatione

$$\Pi=0,$$

petatur ipsius x expressio per reliquas variabiles x_1, x_2, ... x_n: notum est eam fieri solutionem alterius aequationis differentialis partialis,

$$X=X_1\frac{\partial x}{\partial x_1}+X_2\frac{\partial x}{\partial x_2}\,\ldots\,+X_n\frac{\partial x}{\partial x_n}.$$

Unde haec aequatio differentialis partialis ad aequationem differentialem partialem propositam revocari potest. Porro ad aequationis differentialis partialis propositae solutionem constat revocari posse integrationem completam systematis aequationum differentialium vulgarium primi ordinis inter $n+1$ variabiles x, x_1, ... x_n, quod repraesentemus proportionibus,

$$dx:dx_1\,\ldots\,:dx_n=X:X_1:\ldots:X_n.$$

Videlicet si aequationis differentialis partialis propositae solutiones, a se independentes, sunt f_1, f_2, ... f_n, obtinentur aequationes, quibus illud aequationum differentialium vulgarium systema complete integratur, aequando solutiones illas Constantibus Arbitrariis. Et vice versa, si ex aequationibus Integralibus completis petuntur variabilium functiones Constantibus Arbitrariis a se independentibus aequales, ab iisdemque Constantibus Arbitrariis ipsae vacuae: hae functiones erunt aequationis differentialis partialis propositae solutiones a se independentes. Propter hunc trium problematum consensum Multiplicatorem M ad tria illa problemata perinde refero. Qua de re *ipsum M perinde appellabo Multiplicatorem huius aequationis differentialis partialis,*

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\,\ldots\,+X_n\frac{\partial f}{\partial x_n}=0,$$

vel huius,

$$0=X-X_1\frac{\partial x}{\partial x_1}-X_2\frac{\partial x}{\partial x_2}\,\ldots\,-X_n\frac{\partial x}{\partial x_n},$$

vel etiam systematis aequationum differentialium vulgarium,

$$dx:dx_1:dx_2\,\ldots\,:dx_n=X:X_1:X_2:\ldots:X_n.$$

Ubi ad has refertur Multiplicator, quod plerumque usu venit, pro variis formis, quibus earum aequationes integrales completae proponuntur, variae obtinentur Multiplicatoris repraesentationes. Quas sequentibus exponam.

Si aequationes integrales proponuntur ipsa forma cuius modo mentionem iniecimus,

$$5.\quad f_1 = \alpha_1,\quad f_2 = \alpha_2,\quad \ldots\ldots\ f_n = \alpha_n,$$

designantibus α_1 etc. Constantes Arbitrarias, functiones f_1 etc. non afficientes, ideoque $f_1, f_2, \ldots\ldots f_n$ solutiones a se independentes aequationis,

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\ldots\ldots+X_n\frac{\partial f}{\partial x_n}=0,$$

erat Multiplicator,

$$6.\quad M=\frac{1}{X}\Sigma\pm\frac{\partial f_1}{\partial x_1}\cdot\frac{\partial f_2}{\partial x_2}\ldots\ldots\frac{\partial f_n}{\partial x_n}.$$

Iam vero proponantur aequationes integrales completae hac forma maxime usitata, ut variabiles omnes per earum unam veluti x, et Constantes Arbitrarias exprimantur,

$$7.\quad x_1=\varphi_1(x),\quad x_2=\varphi_2(x),\quad \ldots\ldots\ x_n=\varphi_n(x),$$

functionibus φ_1, φ_2 etc. involventibus praeter variabilem x Constantes Arbitrarias α_1 etc., erit

$$8.\quad \Sigma\pm\frac{\partial f_1}{\partial x_1}\cdot\frac{\partial f_2}{\partial x_2}\ldots\ldots\frac{\partial f_n}{\partial x_n}=\frac{1}{\Sigma\pm\frac{\partial\varphi_1}{\partial\alpha_1}\cdot\frac{\partial\varphi_2}{\partial\alpha_2}\ldots\ldots\frac{\partial\varphi_n}{\partial\alpha_n}},$$

D. F. §. 9. (3.) *). Unde fit,

$$9.\quad M=\frac{1}{X\Sigma\pm\frac{\partial\varphi_1}{\partial\alpha_1}\cdot\frac{\partial\varphi_2}{\partial\alpha_2}\ldots\ldots\frac{\partial\varphi_n}{\partial\alpha_n}}=\frac{1}{X\Sigma\pm\frac{\partial x_1}{\partial\alpha_1}\cdot\frac{\partial x_2}{\partial\alpha_2}\ldots\ldots\frac{\partial x_n}{\partial\alpha_n}}.$$

Si vero generalius inter omnes $2n+1$ quantitates, $x, x_1, \ldots\ldots x_n$ $\alpha_1, \alpha_2, \ldots\ldots \alpha_n$, proponuntur n aequationes integrales,

$$\Pi_1=0,\quad \Pi_2=0,\quad \ldots\ldots\ \Pi_n=0,$$

fit (D. F. §. 10. (5.)),

$$10.\quad \Sigma\pm\frac{\partial f_1}{\partial x_1}\cdot\frac{\partial f_2}{\partial x_2}\ldots\ldots\frac{\partial f_n}{\partial x_n}=\frac{(-1)^n\Sigma\pm\frac{\partial\Pi_1}{\partial x_1}\cdot\frac{\partial\Pi_2}{\partial x_2}\ldots\ldots\frac{\partial\Pi_n}{\partial x_n}}{\Sigma\pm\frac{\partial\Pi_1}{\partial\alpha_1}\cdot\frac{\partial\Pi_2}{\partial\alpha_2}\ldots\ldots\frac{\partial\Pi_n}{\partial\alpha_n}}.$$

Unde obtinetur, rejecto quod licet signo ancipiti,

$$11.\quad M=\frac{1}{X}\cdot\frac{\Sigma\pm\frac{\partial\Pi_1}{\partial x_1}\cdot\frac{\partial\Pi_2}{\partial x_2}\ldots\ldots\frac{\partial\Pi_n}{\partial x_n}}{\Sigma\pm\frac{\partial\Pi_1}{\partial\alpha_1}\cdot\frac{\partial\Pi_2}{\partial\alpha_2}\ldots\ldots\frac{\partial\Pi_n}{\partial\alpha_n}},$$

quae est Multiplicatoris expressio maxime generalis.

Formula (10.) ope investigatio valoris Determinantis functionalis haud raro egregie expeditur. Transponamus ex. gr. Constantes Arbitrarias in alte-

*) Commentationem de Determinantibus Functionalibus Vol. XXII Diarii Crelliani insertam designabo per D. F.

ram partem aequationum (1.), atque pro quolibet ipsius i valore statuamus unctionem Π_i aequalem functioni $f_i - \alpha_i$, quocunque modo per aequationes,

$$f_{i+1} = \alpha_{i+1}, \quad f_{i+2} = \alpha_{i+2}, \quad \ldots\ldots \quad f_n = \alpha_n,$$

transformatae. Poterit in locum cuiusque aequationis $f_i = \alpha_i$ adhiberi aequatio $\Pi_i = 0$, unde systema aequationum sequentium,

$$\Pi_1 = 0, \quad \Pi_2 = 0, \quad \ldots\ldots \quad \Pi_n = 0,$$

haberi poterit pro aequationum integralium completarum systemate. Quae ita sunt comparatae aequationes, ut quaelibet functio Π_i non involvat quantitates $\alpha_1, \alpha_2, \ldots\ldots \alpha_{i-1}$, quantitatem α_i autem in unico termino addito $-\alpha_i$. Unde erit

$$\frac{\partial \Pi_i}{\partial \alpha_1} = \frac{\partial \Pi_i}{\partial \alpha_2} \ldots\ldots = \frac{\partial \Pi_i}{\partial \alpha_{i-1}} = 0, \quad \frac{\partial \Pi_i}{\partial \alpha_i} = -1,$$

sive quantitatibus $\frac{\partial \Pi_i}{\partial \alpha_k}$ in figuram quadratam dispositis hunc in modum,

$$\begin{array}{cccc} \frac{\partial \Pi_1}{\partial \alpha_1}, & \frac{\partial \Pi_1}{\partial \alpha_2}, & \ldots\ldots & \frac{\partial \Pi_1}{\partial \alpha_n}, \\ \frac{\partial \Pi_2}{\partial \alpha_1}, & \frac{\partial \Pi_2}{\partial \alpha_2}, & \ldots\ldots & \frac{\partial \Pi_2}{\partial \alpha_n}, \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial \Pi_n}{\partial \alpha_1}, & \frac{\partial \Pi_n}{\partial \alpha_2}, & \ldots\ldots & \frac{\partial \Pi_n}{\partial \alpha_n}, \end{array}$$

quadratoque per diagonalem, a laeva ad dextram partem ductam, in duas partes diviso, termini in laeva parte positi omnes evanescunt. Quod ubi fit, abit Determinans in productum terminorum in ipsa diagonali positorum. Qui termini cum singuli fiant -1, eruitur

$$\Sigma \pm \frac{\partial \Pi_1}{\partial \alpha_1} \cdot \frac{\partial \Pi_2}{\partial \alpha_2} \ldots\ldots \frac{\partial \Pi_n}{\partial \alpha_n} = \pm 1,$$

ideoque

$$12. \quad XM = \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \ldots\ldots \frac{\partial f_n}{\partial x_n}$$
$$= \Sigma \pm \frac{\partial \Pi_1}{\partial x_1} \cdot \frac{\partial \Pi_2}{\partial x_2} \ldots\ldots \frac{\partial \Pi_n}{\partial x_n}.$$

Quae docet formula propositionem frequentissimae applicationis, *valentibus aequationibus $f_1 = \alpha_1$, $f_2 = \alpha_2$, $\ldots\ldots$ $f_n = \alpha_n$, Determinans functionale,*

$$\Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \ldots\ldots \frac{\partial f_n}{\partial x_n},$$

valorem non mutare, si ante differentiationes partiales transigendas quaeque functio f_i per aequationes

$$f_{i+1} = \alpha_{i+1}, \quad f_{i+2} = \alpha_{i+2}, \quad \ldots\ldots \quad f_n = \alpha_n,$$

quascunque subeat mutationes. In hac propositione sunt α_1, α_2, ... α_n Constantes; quae si iunguntur functionibus f_1, f_2, ... f_n, ita ut ipsius $f_i - \alpha_i$ loco scribatur f_i, refertur propositio ad valorem quem induit Determinans functionale, functionibus ipsis evanescentibus. In applicatione huius propositionis facienda functiones f_1, f_2, ... f_n sive aequationes, $f_1 = 0$, $f_2 = 0$, ... $f_n = 0$, certo disponendae sunt ordine tali, ut quaeque aequatio $f_i = 0$ insequentium ope formam induere possit concinnam, simulque differentialia partialia functionis f_i evadant simplicissima. Quin adeo eandem operationem indefinite repetere licet, siquidem post idoneas mutationes, pro certo functionum et aequationum ordine factas, eaedem functiones alio semperque alio ordine disponuntur et pro quaque nova dispositione mutationes vel eliminationes convenientes operantur. Quantascunque autem mutationes per varias istas dispositiones et eliminationes subire possunt functiones propositae f_1 etc., non tamen inde nascuntur functionum mutationis quae obtineri possunt, si *eodem tempore* ad unamquamque transformandam, nullo ordinis functionum respectu habito, omnes adhibentur n aequationes, quae reliquas omnes functiones nihilo aequando proveniunt. Nam in propositione tradita unica tantum erat e $n+1$ functionibus, ad quam transformandam adhiberi poterant n aequationes; praeter hanc una tantum erat ad quam transformandam $n-1$ aequationes adhiberi poterat, et ita porro. Functionibus in alium aliumque ordinem dispositis et pro quaque nova dispositione propositionis traditae applicatione facta, effici quidem potest ut unaquaeque functio sua vice adiumento n aequationum transmutetur; sed differentia in eo constituitur, quod hac ratione aequationes ad transmutationes adhibendae non amplius proveniant nihilo aequando functiones propositas sed functiones et ipsas iam transmutatas. Veluti si f per aequationem $f_1 = 0$ mutatur in φ, ac deinde f_1 per aequationem $\varphi = 0$ in φ_1: ipsa φ_1 non easdem induere potest formas, in quas mutari potest f_1 nihilo aequando ipsam functionem propositam f. Nam si valorem generalem functionis, in quam f per aequationem $f_1 = 0$ mutari potest, designamus quod licet per

$$\varphi = f + \lambda f_1,$$

atque similiter valorem generalem functionis, in quam f_1 per aequationem $\varphi = 0$ mutatur, per

$$\varphi_1 = f_1 + \mu\varphi = (1+\lambda\mu) f_1 + \mu f:$$

haec functio diversa erit a functione $f_1 + \mu\varphi$, in quam f_1 per aequationem $f = 0$ mutatur. Atque Determinans functionum φ et φ_1 idem quidem erit atque functionum propositarum; functionum vero $f + \lambda f_1$, $f_1 + \mu f$ ab illo discre-

pabit, scilicet aequabitur Determinanti functionum f et f_1, per factorem $1-\lambda\mu$ multiplicato. Quod pluribus illustrare placuit, ut emendarem errorem quem in Commentatione *de Determinantibus functionalibus* commisi proponendo, Determinantis functionalis valorem quem induat ipsis functionibus evanescentibus, immutatum manere, si unaquaeque functio mutationes subeat, quascunque nihilo aequando reliquas omnes subire possit. Generaliter si ponitur

$$\varphi_i = \lambda^i f + \lambda_1^i f_1 \ldots + \lambda_n^i f_n,$$

demonstrabitur per Determinantium proprietates, valentibus aequationibus

$$f = 0, \quad f_1 = 0, \quad \ldots \quad f_n = 0,$$

fieri

$$\Sigma \pm \frac{\partial \varphi}{\partial x} \cdot \frac{\partial \varphi_1}{\partial x_1} \ldots \frac{\partial \varphi_n}{\partial x_n} = \Sigma + \lambda \lambda_1' \lambda_2'' \ldots \lambda_n^n . \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \ldots \frac{\partial f_n}{\partial x_n}.$$

Unde ut Determinantia functionum $f, f_1, \ldots f_n$ et $\varphi, \varphi_1, \ldots \varphi_n$ inter se aequalia existant, habetur conditio generalis,

$$\Sigma \pm \lambda \lambda_1' \ldots \lambda_n^n = 1.$$

E Propositione supra tradita, identidem pro aliis aliisque functionum dispositionibus repetita, innumera deducuntur quantitatum λ_k^i systemata quae conditioni illi satisfaciunt.

Inter mutationes, quas functio variabilium x, x_1 etc. per aequationes inter easdem variabiles positas subire potest, referri potest eliminatio variabilium numeri numero aequationum aequalis. Unde in formula (12.) definire licet Π_i ut functionem variabilium $x, x_1, \ldots x_i$, in quam abeat $f_i - \alpha_i$, si ope aequationum $f_{i+1} = \alpha_{i+1}$, $f_{i+2} = \alpha_{i+2}$, $\ldots f_n = \alpha_n$ variabiles $x_{i+1}, x_{i+2}, \ldots x_n$ eliminantur. Quo statuto, omnia evanescunt differentialia partialia $\frac{\partial \Pi_i}{\partial x_k}$, in quibus $k > i$; unde figura quadrata, quae a quantitatibus $\frac{\partial \Pi_i}{\partial x_k}$ formatur, ita comparata erit, ut in ea per diagonalem divisa, rursus termini in altera parte positi evanescant, ideoque fiat,

$$\Sigma \pm \frac{\partial \Pi_1}{\partial x_1} \cdot \frac{\partial \Pi_2}{\partial x_2} \ldots \frac{\partial \Pi_n}{\partial x_n} = \frac{\partial \Pi_1}{\partial x_1} \cdot \frac{\partial \Pi_2}{\partial x_2} \ldots \frac{\partial \Pi_n}{\partial x_n}.$$

Hinc formula (12.) abit in hanc,

$$13. \qquad XM = \frac{\partial \Pi_1}{\partial x_1} \cdot \frac{\partial \Pi_2}{\partial x_2} \ldots \frac{\partial \Pi_n}{\partial x_n},$$

sive Determinans functionale quo Multiplicator definitur in simplex productum redit. Forma autem aequationum integralium

$$\Pi_1 = 0, \quad \Pi_2 = 0, \quad \ldots \quad \Pi_n = 0,$$

quae illam simplicem Determinantis functionalis expressionem suppeditat, eadem

est atque per integrationem *successivam* proveniens, post quodque Integrale inventum una variabilium eliminata. Servata enim functionum Π_1, Π_2, ... Π_n significatione antecedente, si eliminatur x_n per Integrale,

$$\Pi_n = f_n - \alpha_n = 0,$$

erit $\Pi_{n-1} = 0$ Integrale aequationum differentialium,

$$dx : dx_1 \ldots : dx_{n-1} = X : X_1 \ldots : X_{n-1},$$

cuius Integralis ope eliminata x_{n-1} erit $\Pi_{n-2} = 0$ Integrale aequationum differentialium,

$$dx : dx_1 \ldots : dx_{n-2} = X : X_1 \ldots : X_{n-2},$$

et ita porro. Si e functione Π_i Constantes arbitrarias α_{i+1}, α_{i+2}, ... α_n, quas implicat, ope aequationum,

$$\Pi_{i+1} = 0, \quad \Pi_{i+2} = 0, \ldots \quad \Pi_n = 0,$$

eliminamus, redit aequatio $\Pi_i = 0$ in aequationum differentialium propositarum Integrale $f_i - \alpha_i = 0$. Voco autem, ut in aliis Commentationibus, *Integrale systematis aquationum differentialium vulgarium huiusmodi aequationem integralem, quae differentiata identica evadat per solas aequationes differentiales propositas, neque ipsa illa aequatione integrali neque ulla alia in auxilium advocata.*

Multiplicatoris expressio generalis. Bini Multiplicatores suppeditant Integrale. Expressio generalis functiouum quarum detur Determinans datum.

§. 4.

Iam varias quae de Multiplicatore nostro tradi possunt proprietates exponam. Ac primum inquiram quomodo uno cognito Multiplicatore eruantur alii innumeri, sive Multiplicatoris investigabo formam generalem. Sit M datus Multiplicator aequationis,

$$1. \quad X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1} \ldots + X_n\frac{\partial f}{\partial x_n} = 0,$$

satisfacere debet M secundum §. pr. huiusmodi aequationi,

$$2. \quad MX = \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \ldots \frac{\partial f_n}{\partial x_n},$$

designantibus f_1, f_2, ... f_n solutiones aequationis (1.) a se invicem indepentes. Sit μ alius quicunque Multiplicator, satisfaciens aequationi,

$$3. \quad \mu X = \Sigma \pm \frac{\partial F_1}{\partial x_1} \cdot \frac{\partial F_2}{\partial x_2} \ldots \frac{\partial F_n}{\partial x_n},$$

designantibus F_1, F_2, ... F_n aliud systema solutionum eiusdem aequationis (1.) a se invicem independentium. Functiones F_1, F_2, etc. esse debent

solarum $f_1, f_2, \ldots. f_n$ functiones; cognitis enim aequationis (1.) solutionibus n a se invicem independentibus, quaevis alia eiusdem aequationis solutio harum n solutionum functio est. Fit autem per formulam notam (D. F. §. 11. Prop. II.),

$$4. \quad \Sigma \pm \frac{\partial F_1}{\partial x_1} \cdot \frac{\partial F_2}{\partial x_2} \cdots \frac{\partial F_n}{\partial x_n} = \Sigma \pm \frac{\partial F_1}{\partial f_1} \cdot \frac{\partial F_2}{\partial f_2} \cdots \frac{\partial F_n}{\partial f_n} \cdot \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n},$$

siquidem habentur $F_1, F_2, \ldots. F_n$ in laeva formulae parte pro variabilium $x, x_1, \ldots. x_n$ functionibus, in dextra parte pro functionibus ipsarum $f_1, f_2, \ldots. f_n$. E (2.) — (4.) autem obtinetur haec formula,

$$5. \quad \mu = M \Sigma \pm \frac{\partial F_1}{\partial f_1} \cdot \frac{\partial F_2}{\partial f_2} \cdots \frac{\partial F_n}{\partial f_n}.$$

Unde sequitur vice versa, ipsarum $f_1, f_2, \ldots. f_n$ quibuscunque sumtis functionibus a se independentibus $F_1, F_2, \ldots. F_n$, Multiplicatorem M ductum in harum functionum Determinans,

$$\Sigma \pm \frac{\partial F_1}{\partial f_1} \cdot \frac{\partial F_2}{\partial f_2} \cdots \frac{\partial F_n}{\partial f_n},$$

alterum suppeditare Multiplicatorem μ. Quaecunque enim sint $F_1, F_2, \ldots. F_n$ ipsarum $f_1, f_2, \ldots. f_n$ functiones a se independentes, ex aequationibus (2.), (4.), (5.) sequitur formula (3.), in qua $F_1, F_2, \ldots. F_n$ erunt aequationis (1.) solutiones a se invicem independentes, unde secundum §. pr. tradito quantitas μ, formula (3.) determinata, aequationis (1.) erit Multiplicator.

Videmus ex antecedentibus, binorum quorumque Multiplicatorum Quotientem $\frac{\mu}{M}$ aequari functioni ipsarum $f_1, f_2, \ldots. f_n$, videlicet Determinanti ipsarum $F_1, F_2, \ldots. F_n$, pro functionibus quantitatum $f_1, f_2, \ldots. f_n$ habitarum, et vice versa, Multiplicatore M ducto in Determinans quarumcunque n functionum a se independentium quantitatum $f_1, f_2, \ldots. f_n$, alterum obtineri Multiplicatorem. Semper autem quantitatum $f_1, f_2, \ldots. f_n$ functiones $F_1, F_2, \ldots. F_n$ invenire licet, quarum Determinans sit earundem quantitatum data quaecunque functio. Unde non modo binorum Multiplicatorum M et μ Quotiens functioni aequatur ipsarum $f_1, f_1, \ldots. f_n$, sed etiam vice versa, Multiplicatore M in quamcunque functionem ipsarum $f_1, f_2, \ldots. f_n$ ducto, rursus prodit Multiplicator. Et eum ipsarum, $f_1, f_2, \ldots. f_n$, quaelibet functio aequationis (1.) solutio sit, neque aliae aequationis (1.) solutiones extare possint, nisi quae ipsarum $f_1, f_2, \ldots. f_n$ functiones sint, sequitur ex antecedentibus haec Propositio.

Propositio.

„Designante M Multiplicatorem aequationis differentialis partialis,

$$X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}=0,$$

erit Multiplicatoris forma generalis,

$$\Pi M,$$

designante Π quamcunque aequationis propositae solutionem."

Cognita aequationis (1.) solutione Π ac designante α Constantem Arbitrariam, aequatione $\Pi=\alpha$ determinatur variabilium $x_1, x_2, \dots x_n$ functio x, satisfaciens aequationi differentiali partiali,

$$6.\quad 0=X-X_1\frac{\partial x}{\partial x_1}-X_2\frac{\partial x}{\partial x_2}\dots-X_n\frac{\partial x}{\partial x_n},$$

nec non erit $\Pi=\alpha$ Integrale aequationum differentialium vulgarium simultanearum,

$$7.\quad dx:dx_1\dots:dx_n=X:X_1\dots:X_n.$$

Unde Propositio antecedens docet, *cognitis aequationis differentialis partialis* (6.) *vel aequationum* (7.) *differentialium vulgarium binis Multiplicatoribus M et M_1, non solo factore constante inter se diversis, aequationem*

$$\frac{M_1}{M}=\text{Const.}$$

fore aequationis differentialis partialis (6.) *solutionem vel systematis aequationum differentialium* (7.) *Integrale.*

Pluribus datis Multiplicatoribus $M, M_1, \dots M_k$, haec quoque quantitas,

$$MF\left(\frac{M_1}{M}, \frac{M_2}{M}, \dots \frac{M_k}{M}\right)$$

erit multiplicator. Designante enim F ipsarum $\frac{M_1}{M}$ etc. functionem arbitrariam, non tantum fractiones $\frac{M_1}{M}$, $\frac{M_2}{M}$ etc., sed ipsa F quoque aequationis (1.) solutio fit. Unde etiam aequatione $F=0$ sive quod idem est *quacunque aequatione homogenea inter datos Multiplicatores posita determinatur aequationis* (6.) *solutio.* Nec non designantibus $\alpha_1, \alpha_2, \dots \alpha_n$ Constantes Arbitrarias, erunt

$$\frac{M_1}{M}=\alpha_1,\quad \frac{M_2}{M}=\alpha_2,\ \dots\ \frac{M_k}{M}=\alpha_k,$$

Integralia aequationum differentialium vulgarium (7.).

Restat, ut paucis exponam quomodo inveniantur functiones quarum Determinans datae variabilium functioni aequetur, quod semper fieri posse supra

innui. Immo videbimus idem innumeris modis succedere, videlicet functiones praeter unam omnes ex arbitrio sumi posse, una reliqua per solam Quadraturam determinata.

Designante Π datam quamcunque quantitatum $f_1, f_2, \ldots f_n$ functionem, simplicissima habetur solutio aequationis,

$$8. \quad \Sigma \pm \frac{\partial F_1}{\partial f_1} \cdot \frac{\partial F_2}{\partial f_2} \cdots \frac{\partial F_n}{\partial f_n} = \Pi,$$

ponendo,

$$F_2 = f_2, \quad F_3 = f_3, \quad \ldots \quad F_n = f_n,$$

unde Determinans propositum in simplex differentiale abit,

$$\frac{\partial F_1}{\partial f_1} = \Pi.$$

Quo igitur casu fit,

$$F_1 = \int \Pi df_1,$$

cui integrali functionem ipsarum $f_2, f_3, \ldots f_n$ arbitrariam addere licet, quippe quae inter integrationem pro Constantibus habentur. Aequationis (8.) solutio generalis obtinetur sequenti modo. Pro ipsis $F_2, F_3, \ldots F_n$ ex arbitrio sumantur ipsarum $f_1, f_2, \ldots f_n$ functiones a se independentes, atque fingatur, reliquam functionem F_1 exhiberi per quantitates,

$$f_1, \quad F_2, \quad F_3, \quad \ldots \quad F_n.$$

Functionis F_1 hoc modo repraesentatae differentialia partialia uncis includam, quo distinguantur a differentialibus eiusdem functionis per $f_1, f_2, \ldots f_n$ exhibitae, ita ut sit,

$$\frac{\partial F_1}{\partial f_1} = \left(\frac{\partial F_1}{\partial f_1}\right) + \left(\frac{\partial F_1}{\partial F_2}\right)\frac{\partial F_2}{\partial f_1} + \left(\frac{\partial F_1}{\partial F_3}\right)\frac{\partial F_3}{\partial f_1} \cdots + \left(\frac{\partial F_1}{\partial F_n}\right)\frac{\partial F_n}{\partial f_1},$$

et quoties index i ab unitate diversus est,

$$\frac{\partial F_1}{\partial f_i} = \left(\frac{\partial F_1}{\partial F_2}\right)\frac{\partial F_2}{\partial f_i} + \left(\frac{\partial F_1}{\partial f_3}\right)\frac{\partial F_3}{\partial f_i} \cdots + \left(\frac{\partial F_1}{\partial F_n}\right)\frac{\partial F_n}{\partial f_i}.$$

Quae ipsarum

$$\frac{\partial F_1}{d f_1}, \quad \frac{\partial F_1}{\partial f_2}, \quad \ldots \quad \frac{\partial F_1}{\partial f_n}$$

expressiones si substituuntur in Determinante,

$$\Sigma \pm \frac{\partial F_1}{\partial f_1} \cdot \frac{\partial F_2}{\partial f_2} \cdots \frac{\partial F_n}{\partial f_n},$$

identice evanescunt singula aggregata per singula differentialia partialia

$$\left(\frac{\partial F_1}{\partial F_2}\right), \quad \left(\frac{\partial F_1}{\partial F_3}\right), \quad \ldots \quad \left(\frac{\partial F_1}{\partial F_n}\right)$$

multiplicatae, unde simplex formula obtinetur,

$$9.\quad \Sigma\pm\frac{\partial F_1}{\partial f_1}\cdot\frac{\partial F_2}{\partial f_2}\cdots\cdots\frac{\partial F_n}{\partial f_n} = \left(\frac{\partial F_1}{\partial f_1}\right)\Sigma\pm\frac{\partial F_2}{\partial f_2}\cdot\frac{\partial F_3}{\partial f_3}\cdots\cdots\frac{\partial F_n}{\partial f_n}$$

D. F. §. 12. (4.)). E (8. et 9.) sequitur

$$\left(\frac{\partial F_1}{\partial f_1}\right) = \frac{\Pi}{\Sigma\pm\frac{\partial F_2}{\partial f_2}\cdot\frac{\partial F_3}{\partial f_3}\cdots\cdots\frac{\partial F_n}{\partial f_n}},$$

qua formula exprimendo $f_2, f_3, \ldots. f_n$ per $f_1, F_2, F_3, \ldots. F_n$, sic quoque exhiberi potest,

$$10.\quad \left(\frac{\partial F_1}{\partial f_1}\right) = \Pi\Sigma\pm\frac{\partial f_2}{\partial F_2}\cdot\frac{\partial f_3}{\partial F_3}\cdots\cdots\frac{\partial f_n}{\partial F_n}$$

(D. F. §. 9. (3.)). Secundum hanc formulam, ut modo maxime generali variabilium $f_1, f_2, \ldots. f_n$ inveniantur functiones, quarum Determinans datae earundem variabilium functioni Π aequatur, ex arbitrio exprimantur $f_2, f_3, \ldots. f_n$ per f_1 aliasque $n-1$ quantitates $F_2, F_3, \ldots. F_n$, determinataque F_1 per formulam,

$$11.\quad F_1 = \int \Pi\Sigma\pm\frac{\partial f_2}{\partial F_2}\cdot\frac{\partial f_3}{\partial F_3}\cdots\cdots\frac{\partial f_n}{\partial F_n}\,\partial f_1,$$

ipsae $F_1, F_2, \ldots. F_n$, vice versa per $f_1, f_2, \ldots. f_n$ expressae erunt functiones quaesitae.

Ponendo $\Pi = 1$ antecedentibus innumera obtinentur systemata functionum quantitatum $f_1, f_2, \ldots. f_n$, quarum Determinans unitati aequatur. Quibus omnibus idem respondet Multiplicator. Quoties enim

$$\Sigma\pm\frac{\partial F_1}{\partial f_1}\cdot\frac{\partial F_2}{\partial f_2}\cdots\cdots\frac{\partial F_n}{\partial f_n} = 1,$$

sequitur e (5.)

$$\mu = M.$$

Vice versa, si idem Multiplicator respondet binis systematis n solutionum a se independentium aequationis differentialis partialis (1.), $f_1, f_2, \ldots. f_n$ atque $F_1, F_2, \ldots. F_n$, ita ut sit,

$$\begin{aligned} MX &= \Sigma\pm\frac{\partial f_1}{\partial x_1}\cdot\frac{\partial f_2}{\partial x_2}\cdots\cdots\frac{\partial f_n}{\partial x_n} \\ &= \Sigma\pm\frac{\partial F_1}{\partial x_1}\cdot\frac{\partial F_2}{\partial x_2}\cdots\cdots\frac{\partial F_n}{\partial x_n}: \end{aligned}$$

erunt $F_1, F_2, \ldots. F_n$ quantitatum $f_1, f_2, \ldots. f_n$ functiones, quarum Determinans unitati aequatur.

Multiplicatoris definitio per aequationem differentialem partialem. Conditio, ut Multiplicator aequari possit unitati.

§. 5.

Vidimus §. 3. aequationis differentialis partialis,

$$1. \quad X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}=0,$$

Multiplicatorem quemcunque M alii satisfacere aequationi differentiali partiali,

$$2. \quad \frac{\partial .MX}{\partial x}+\frac{\partial .MX_1}{\partial x_1}\dots+\frac{\partial .MX_n}{\partial x_n}.$$

Vice versa *quaecunque habetur solutio* μ *aequationis differentialis partialis,*

$$3. \quad \frac{\partial .\mu X}{\partial x}+\frac{\partial .\mu X_1}{\partial x_1}\dots+\frac{\partial .\mu X_n}{\partial x_n}=0,$$

erit illa aequationis (1.) *Multiplicator.*

Ponamus enim $\mu=\Pi.M$, abit aequatio (3.) in sequentem,

$$0=\Pi\left(\frac{\partial .MX}{\partial x}+\frac{\partial .MX_1}{\partial x_1}\dots+\frac{\partial .MX_n}{\partial x_n}\right)$$
$$+M\left(X\frac{\partial \Pi}{\partial x}+X_1\frac{\partial \Pi}{\partial x_1}\dots+X_n\frac{\partial \Pi}{\partial x_n}\right).$$

Partis dextrae Aggregatum in Π ductum secundum (2.) evanescit; unde, cum supponamus ipsum M non evanescere, sequitur,

$$0=X\frac{\partial \Pi}{\partial x}+X_1\frac{\partial \Pi}{\partial x_1}\dots+X_n\frac{\partial \Pi}{\partial x_n}.$$

Erit igitur Π aequationis (1.) solutio ideoque secundum Propositionem §. pr. traditam, Multiplicatorem in solutionem aequationis (1.) quamcunque ductum reproducere Multiplicatorem, erit $\Pi.M=\mu$ Multiplicator, q. d. e.

Cum quilibet Multiplicator sit solutio aequationis (3.) et secundum antecedentia quaelibet aequationis (3.) solutio sit Multiplicator, poterit aequatio (3.) adhiberi ad Multiplicatorem definiendum. Habemus igitur Propositionem sequentem.

Propositio I.

„Designante M solutionem quamcunque aequationis differentialis partialis,

$$\frac{\partial .MX}{\partial x}+\frac{\partial .MX_1}{\partial x_1}\dots+\frac{\partial .MX_n}{\partial x_n}=0,$$

semper dantur functiones $f_1, f_2, \dots f_n$, quae pro functione f indefinita efficiant aequationem,

$$M\left(X\frac{\partial f}{\partial x}+X_1\frac{\partial f}{\partial x_1}\dots+X_n\frac{\partial f}{\partial x_n}\right)=\Sigma\pm\frac{\partial f}{\partial x}\cdot\frac{\partial f_1}{\partial x_1}\dots\frac{\partial f_n}{\partial x_n}."$$

Videri possit parum lucri percipi e nova Multiplicatoris determinatione per aequationem differentialem partialem (3.). Aequationis (3.) enim solutio generalis non habetur nisi aequationis (1.) data sit solutio generalis sive eius innotescant n solutiones particulares a se invicem independentes. His autem cognitis habetur Multiplicator per formulam (2.) §. pr. At observo ad Multiplicatorem eruendum tantum nos indigere una aliqua solutione particulari aequationis (3.) et quamquam aequationis (3.) solutio generalis a solutione aequationis (1.) pendet et pro complicatiore habenda est, fieri tamen potest ut aequationis (3.) innotescat solutio particularis, dum aequationis (1.) solutiones adhuc omnes ignoramus.

Inter solutiones aequationis differentialis partialis (1.) non referri solet, quae sponte se offert, $f = \text{Const.}$ Sed e solutionibus aequationis (3.) quae Multiplicatorem suggerunt quantitates constantes non excluduntur. Fit autem Multiplicator Constanti vel si placet unitati aequalis, si inter ipsas X, X_1 etc. locum habet aequatio,

$$4. \quad \frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \dots + \frac{\partial X_n}{\partial x_n} = 0.$$

Eo casu ipsa expressio proposita,

$$X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1} \dots + X_n\frac{\partial f}{\partial x_n},$$

pro functione f indefinita aequivalet alicui Determinanti functionali,

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \dots \frac{\partial f_n}{\partial x_n},$$

sive adhibendo notationes §. 3. usitatas statuere licet,

$$X = A, \quad X_1 = A_1, \dots X_n = A_n.$$

Quod, si ea tenes quae §. 2. de Determinantibus functionalibus partialibus monui, sic quoque proponi potest.

Propositio II.

„Si $n+1$ variabilium $x, x_1, \dots x_n$ functiones $X, X_1, \dots X_n$ satisfaciant conditioni,

$$\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} + \frac{\partial X_2}{\partial x_2} \dots + \frac{\partial X_n}{\partial x_n} = 0,$$

ipsae $n+1$ quantitates $X, X_1, \dots X_n$ haberi possunt pro certarum n functionum Determinantibus partialibus."

Haec Propositio analoga est notae elementari, si variabilium x et y functiones X et Y satisfaciant conditioni, $\frac{\partial X}{\partial x} + \frac{\partial Y}{\partial y} = 0$, ipsas Y et $-X$

respective haberi posse pro eiusdem functionis differentialibus partialibus, variabilium x et y respectu sumtis.

Si inter quantitates X, X_1 etc. conditio (4.) locum habet, aequatio differentialis partialis (3.), qua Multiplicator definitur, in ipsam (1.) redit. Eo igitur casu quaecunque aequationis (1.) solutio eiusdem aequationis Multiplicator erit, siquidem iam unitatem vel numeros constantes inter solutiones referimus. Unde etiam patet, eo casu aequationum differentialium vulgarium,

$$dx : dx_1 \dots : dx_n = X : X_1 \dots : X_n,$$

Multiplicatorem fore quantitatem quamcunque, aut per se constantem, aut quae per aequationes integrales completas Constanti aequetur.

Cognito systematis aequationum differentialium vulgarium Multiplicatore quocunque eruuntur Determinantia functionum quae per aequationes integrales completas valoribus variabilium initialibus aequivalent.

§. 6.

Vidimus §. 3. designantibus $f_1, f_2, \dots f_n$ solutiones a se independentes aequationis,

$$1. \quad X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1} + \dots + X_n\frac{\partial f}{\partial x_n} = 0,$$

harum functionum Determinantia partialia $A_1, A_2, \dots A_n$ esse inter se ut aequationis (1.) Coëfficientes, sive fieri,

$$2. \quad A : A_1 \dots : A_n = X : X_1 \dots : X_n.$$

Unde omnia $A_1, A_2, \dots A_n$ uno determinantur A. Antecedentibus autem demonstravi, designante μ Multiplicatorem aequationis (1.) quemcunque sive quamcunque solutionem aequationis

$$3. \quad \frac{\partial . X\mu}{\partial x} + \frac{\partial . X_1\mu}{\partial x_1} \dots + \frac{\partial . X_n\mu}{\partial x_n} = 0,$$

fieri $\mu = \Pi M$, ideoque

$$4. \quad \mu X = \Pi . A = \Pi . \Sigma \pm \frac{\partial f_1}{\partial x_1} . \frac{\partial f_2}{\partial x_2}, \dots \frac{\partial f_n}{\partial x_n},$$

ubi Π certa quaedam est ipsarum $f_1, f_2 \dots f_n$ functio sive aequationis (1.) solutio. Hinc e data quacunque aequationis (3.) solutione μ cognoscitur valor Determinantis A, dummodo determinata erit functio Π. *Eruitur autem functio Π, dummodo Determinantis A innotescat valor quem pro $x = 0$ induit.* Generaliter enim, ut functio f aequationi differentiali partiali (1.) satisfaciens omnino determinata sit, poscitur et sufficit ut aliqua cognoscatur functio, cui illa aequalis evadat ubi inter variabiles $x, x_1, \dots x_n$ data aliqua

aequatio locum habet, veluti si ipsius f datur valor quem pro $x=0$ induit. Hinc si ponimus pro $x=0$ abire μ, X, A in variabilium $x_1, x_2, \dots x_n$ functiones μ^0, X^0, A^0; functio Π eo determinabitur quod esse debeat aequationis (1.) solutio atque pro $x=0$ aequalis evadet variabilium $x_1, x_2, \dots x_n$ functioni

$$\frac{\mu^0 X^0}{A^0}.$$

Eiusmodi solutio autem ut inveniatur sint $f_1^0, f_2^0, \dots f_n^0$ variabilium $x_1, x_2, \dots$ $\dots x_n$ functiones, in quas pro $x=0$ abeunt $f_1, f_2, \dots f_n$; exprimatur porro variabilium $x_1, x_2, \dots x_n$ functio $\frac{\mu^0 X^0}{A^0}$ per $f_1^0, f_2^0, \dots f_n^0$; in qua expressione ponendo ipsarum $f_1^0, f_2^0, \dots f_n^0$ loco ipsas $f_1, f_2, \dots f_n$, prodibit functio quaesita Π. Quippe functio sic inventa erit aequationis (1.) solutio et pro $x=0$ abibit in variabilium $x_1, x_2, \dots x_n$ functionem $\frac{\mu^0 X^0}{A^0}$.

Functionem A^0 casu prae ceteris notando a priori assignare licet, videlicet quoties $f_1, f_2, \dots f_n$ tales sunt aequationis (1.) solutiones *quae pro $x=0$ in ipsas variabiles $x_1, x_2, \dots x_n$ abeunt.* Tunc enim habetur

$$f_1^0 = x_1, \quad f_2^0 = x_2, \quad \dots \quad f_n^0 = x_n,$$

ideoque

$$A^0 = \Sigma \pm \frac{\partial f_1^0}{\partial x_1} \cdot \frac{\partial f_2^0}{\partial x_2} \dots \frac{\partial f_n^0}{\partial x_n} = 1.$$

Hinc secundum regulam traditam functio Π e functione $\mu^0 X^0$ eruitur substituendo variabilibus $x_1, x_2, \dots x_n$ functiones $f_1, f_1, \dots f_n$, sive quod idem est, substituendo in ipsa μX variabilibus $x, x_1, x_2, \dots x_n$ quantitates $0, f_1, f_2, \dots f_n$. Id quod sequentem suppeditat Propositionem.

Propositio I.

„Sint $f_1, f_2, \dots f_n$ solutiones aequationis

$$X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1} \dots + X_n\frac{\partial f}{\partial x_n} = 0,$$

quae pro $x=0$ in ipsas variabiles $x, x_2, \dots x_n$ abeunt; sit μ quantitas quaecunque satisfaciens aequationi

$$\frac{\partial . X\mu}{\partial x} + \frac{\partial . X_1\mu}{\partial x_1} \dots + \frac{\partial . X_n\mu}{\partial x_n} = 0,$$

atque sit Π ipsarum $f_1, f_2, \dots f_n$ functio quae e producto μX provenit substituendo variabilibus $x, x_1, x_2, \dots x_n$ quantitates $0, f_1, f_2, \dots f_n$: erit

$$\Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \dots \frac{\partial f_n}{\partial x_n} = \frac{\mu X}{\Pi},$$

sive generalius, designante f functionem indefinitam, erit

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n} = \frac{\mu}{\Pi} \left\{ X \frac{\partial f}{\partial x} + X_1 \frac{\partial f}{\partial x_1} \cdots + X_n \frac{\partial f}{\partial x_n} \right\}."$$

Observo hac occasione generaliter, datis aequationis (1.) solutionibus f_1, f_2, ... f_n, quae pro $x = 0$ ipsas x_1, x_2, ... x_n abeant, quamvis aliam eiusdem aequationis solutionem Π per ipsas f_1, f_2, ... f_n absque omni eliminationis negotio exhiberi. Scilicet sufficit in functione Π variabilibus x, x_1, x_2, ... x_n substituere quantitates 0, f_1, f_2, ... f_n.

Casu speciali, quem sub finem §. pr. consideravi, posita insuper $X = 1$, e Propositione praecedente emergit haec:

Propositio II.

„Sint f_1, f_2, ... f_n tales solutiones aequationis,

$$\frac{\partial f}{\partial x} + X_1 \frac{\partial f}{\partial x_1} + X_2 \frac{\partial f}{\partial x_2} \cdots + X_n \frac{\partial f}{\partial x_n} = 0,$$

quae pro $x = 0$ respective in x_1, x_2, ... x_n abeant, sitque identice,

$$\frac{\partial X_1}{\partial x_1} + \frac{\partial X_2}{\partial x_2} \cdots + \frac{\partial X_n}{\partial x_n} = 0,$$

erit,

$$\Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n} = 1,$$

atque reliqua functionum f_1, f_2, ... f_n Determinantia partialia A_1, A_2, ... A_n in ipsas redeunt quantitates X_1, X_2, ... X_n."

Convenit Propositiones antecedentibus inventas ad systemata aequationum differentialium vulgarium referre. Proponatur enim systema aequationum differentialium vulgarium,

$$dx : dx_1 : dx_2 \ldots : dx_n = X : X_1 : X_2 \ldots : X_n,$$

eiusque integratione completa facta, pro Constantibus Arbitrariis adhibeantur valores quos x_1, x_2, ... x_n pro $x = 0$ induunt; resolutione deinde aequationum integralium erui poterunt variabilium x, x_1, ... x_n functiones illis Constantibus Arbitrariis aequales, quae ipsae erunt functiones f_1, f_2, ... f_n, in Propp. I. et II. consideratae. Generaliter Integralia completa sint,

$$f_1 = \alpha_1, \quad f_2 = \alpha_2, \quad \ldots . \quad f_n = \alpha_n,$$

designantibus α_1, α_2 etc. Constantes Arbitrarias quascunque, a quibus ipsae f_1, f_2 etc. vacuae supponuntur. Quorum Integralium ope expressis x_1, x_2, ... x_n per x et Constantes Arbitrarias α_1, α_2, ... α_n, fit secundum formulas de Determinantibus functionalibus traditas,

$$A = \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n} = \left\{ \Sigma \pm \frac{\partial x_1}{\partial \alpha_1} \cdot \frac{\partial x_2}{\partial \alpha_2} \cdots \frac{\partial x_n}{\partial \alpha_n} \right\}^{-1}.$$

Unde formula (4.) docet, cognito aequationum differentialium vulgarium propositarum Mulliplicatore aliquo μ, sive aequationis (3.) solutione, fieri

$$\Sigma \pm \frac{\partial x_1}{\partial \alpha_1} \cdot \frac{\partial x_2}{\partial \alpha_2} \cdots \frac{\partial x_n}{\partial \alpha_n} = \frac{C}{\mu X},$$

designante C functionem Constantium Arbitrariarum. Quoties sunt $\alpha_1, \alpha_2, \ldots \alpha_n$ valores initiales variabilium $x_1, x_2, \ldots x_n$, ipsi $x = 0$ respondentes, Determinans functionale, in laeva parte aequationis antecedentis collocatum, ponendo $x = 0$ in *unitatem* abit. Quo igitur casu Constans C ex ipsa μX eruitur ponendo variabilium $x, x_1, x_2, \ldots x_n$ loco valores $0, \alpha_1, \alpha_2, \ldots \alpha_n$. Casu speciali quo Multiplicator unitatem aequat, e Propositione II. eruitur sequens prae ceteris simplex Propositio.

Propositio III.

„Proponantur aequationes differentiales vulgares simultaneae,

$$\frac{\partial x_1}{\partial x} = X_1, \quad \frac{\partial x_2}{\partial x} = X_2, \quad \ldots \quad \frac{\partial x_n}{\partial x} = X_n,$$

in quibus sint $X_1, X_2, \ldots X_n$ tales variabilium $x, x_1, x_2, \ldots x_n$, functiones quae satisfaciant aequationi,

$$\frac{\partial X_1}{\partial x_1} + \frac{\partial X_2}{\partial x_2} \cdots + \frac{\partial X_n}{\partial x_n} = 0;$$

integratione completa expressis $x_1, x_2, \ldots x_n$ per x earumque valores initiales $\alpha_1, \alpha_2, \ldots \alpha_n$, erit non tantum pro $x = 0$, sed pro valore ipsius x indefinito,

$$\Sigma \pm \frac{\partial x_1}{\partial \alpha_1} \cdot \frac{\partial x_2}{\partial \alpha_2} \cdots \frac{\partial x_n}{\partial \alpha_n} = 1."$$

Quae licet a proposito meo aliena utile videbatur obiter adnotare.

Quo rectius intelligantur quae supra monui de definienda solutione f aequationis differentialis partialis (1.), sequentia adiicio. Sit φ functio in quam abire debet f pro aequatione aliqua inter variabiles $x, x_1, \ldots x_n$ data. Si φ et ipsa aequationis (1.) solutio est, erit $f = \varphi$ functio quaesita, quaecunque sit illa aequatio. Si φ non est aequationis (1.) solutio, fieri non debet ut aequatio illa ad aliam inter quantitates $f_1, f_2, \ldots f_n$ revocari possit, sive ut ex aequatione illa peti possit solutio aequationis differentialis partialis,

$$X = X_1 \frac{\partial x}{\partial x_1} + X_2 \frac{\partial x}{\partial x_2} \cdots + X_n \frac{\partial x}{\partial x_n}.$$

Nisi forte eiusmodi solutio sit *singularis* seu non redeat in aequationem inter quantitates $f_1, f_2, \ldots f_n$, quo casu nihil impedit quo minus functio f definiatur

ope valoris quem pro data illa aequatione induit. Infra autem videbimus pro aequationis differentialis partialis antecedentis solutione singulari fieri,

$$\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}=\infty,$$

ubi ipsae X, X_1 etc. cum a factoribus communibus tum a denominatoribus purgatae supponuntur. Ita non definiri poterit f ope valoris quem pro $x=0$ induit, ubi pro $x=0$ habetur $X=0$ nec simul $\frac{\partial X}{\partial x}=\infty$. Quod obiter observo.

Multiplicatoris definitio per aequationem differentialem vulgarem.

§. 7.

Multiplicatorem, quem antecedentibus per aequationem differentialem partialem definivi, etiam per formulam differentialem vulgarem definire licet. Quae nova forma aequationis praeceteris indagando Multiplicatori apta est.

Primum aequationem differentialem partialem, qua Multiplicator μ definitur, sic exhibeo,

$$1.\quad 0=X\frac{\partial\mu}{\partial x}+X_1\frac{\partial\mu}{\partial x_1}\dots+X_n\frac{\partial\mu}{\partial x_n}+\mu\left\{\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}\right\},$$

vel dividendo per μ,

$$2.\quad 0=X\frac{\partial\log\mu}{\partial x}+X_1\frac{\partial\log\mu}{\partial x_1}\dots+X_n\frac{\partial\log\mu}{\partial x_n}+\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}.$$

Per aequationes autem differentiales vulgares quarum μ est Multiplicator,

$$3.\quad dx:dx_1:dx_2\dots:dx_n=X:X_1:X_2\dots:X_n,$$

aequationem praecedentem brevius sic repraesentare licet,

$$4.\quad 0=X\frac{d\log\mu}{dx}+\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}.$$

Hinc poterit aequationum differentialium vulgarium (3.) Multiplicator μ definiri ut *functio quae solarum aequationum differentialium propositarum* (3.) *ope, nulla in auxilium vocata aequatione integrali, aequationi* (4.) *satisfaciat.* Quippe quod fieri non potest nisi μ *identice* satisfaciat aequationi (2.) qua Multiplicator definiebatur.

Sequitur ex antecedentibus, ad investigandum Multiplicatorem circumspiciendum esse, an aequationum differentialium (3.) ope contingat, expressioni

$$\left\{\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}\right\}\frac{dx}{X}$$

formam conciliare alicuius differentialis completi dU. Quippe hoc patrato fit

e (4.) Multiplicator,

$$5.\quad \mu = e^{-\int\left(\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}\right)\frac{dx}{X}} = e^{-U}.$$

Hanc indagandi Multiplicatoris methodum in aliis Commentationibus per varia exempla illustrabo, in quibus integrationem quae Multiplicatorem suggerit videbimus praestari posse, aequationum differentialium vulgarium propositarum nullo Integrali cognito. Esse tamen poterit formulae (4.) usus etiam si aequationes differentiales complete integratae sunt. Tum enim formula (4.) docet, formationi Determinantis functionalis, quam determinatio Multiplicatoris requirebat, substitui posse Quadraturam, minus interdum molestam. Etenim ope integrationis completae quantitas ipsi $\frac{d\log\mu}{dx}$ aequalis per solam x et Constantes Arbitrarias exhiberi potest, unde ipsum $\log\mu$ per Quadraturam obtines,

$$6.\quad \log\mu = -\int\frac{dx}{X}\left(\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}\right).$$

Post integrationem factam substituendo Constantibus Arbitrariis variabilium x, x_1, x_2, ... x_n functiones aequivalentes, prodibit ipsius $\log\mu$ expressio, aequationi differentiali partiali (2.) satisfaciens.

Post aequationum (3.) integrationem completam expressis x_1, x_2, ... x_n per x et Constantes Arbitrarias α_1, α_2, ... α_n fit secundum §. pr.

$$7.\quad \log\Sigma\pm\frac{\partial x_1}{\partial\alpha_1}\cdot\frac{\partial x_2}{\partial\alpha_2}\dots\frac{\partial x_n}{\partial\alpha_n} = \log\frac{C}{\mu X},$$

designante C Constantium Arbitrariarum functionem. Unde, omissa quod licet Constante, e formula (6.) eruitur

$$8.\quad \log\Sigma\pm\frac{\partial x_1}{\partial\alpha_1}\cdot\frac{\partial x_2}{\partial\alpha_2}\dots\frac{\partial x_n}{\partial\alpha_n} = \log\frac{1}{X}+\int\frac{dx}{X}\left(\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}\right).$$

Quae formula immutata manere debet, omnibus X, X_1, ... X_n per factorem quemcunque communem multiplicatis. Quod ut pateat observo, per aequationes differentiales vulgares propositas aequationem (4.) aucta symmetria sic proponi posse:

$$9.\quad 0 = d\log\mu+\frac{\partial\log X}{\partial x}dx+\frac{\partial\log X_1}{\partial x_1}dx_1\dots+\frac{\partial\log X_n}{\partial x_n}dx_n.$$

Unde e formula (7.) eruitur:

$$\log\Sigma\pm\frac{\partial x_1}{\partial\alpha_1}\cdot\frac{\partial x_2}{\partial\alpha_2}\dots\frac{\partial x_n}{\partial\alpha_n} = \log\frac{C}{\mu X}$$

$$= \log\frac{1}{X}+\int\left(\frac{\partial\log X}{\partial x}dx+\frac{\partial\log X_1}{\partial x_1}dx_1\dots+\frac{\partial\log X_n}{\partial x_n}dx_n\right).$$

Si in hac formula simul omnes X, X_1 etc. in factorem communem ν ducuntur, augetur integrale quantitate,

$$\int\left(\frac{\partial \log \nu}{\partial x} dx + \frac{\partial \log \nu}{\partial x_1} dx_1 \ldots + \frac{\partial \log \nu}{\partial x_n} dx_n\right) = \int d\log\nu = \log\nu.$$

Eadem autem quantitate minuitur $\log\frac{1}{X}$, unde tota expressio immutata manet, q. d. e.

Si in formula (8.) ponimus $X = 1$, prodit Propositio sequens.

Propositio.

„Facta integratione completa aequationum differentialium vulgarium,

$$\frac{dx_1}{dx} = X_1, \quad \frac{dx_2}{dx} = X_2, \quad \ldots\ldots \quad \frac{dx_n}{dx} = X_n,$$

exhibeantur $x_1, x_2, \ldots. x_n$ per x et Constantes Arbitrarias, $\alpha_1, \alpha_2, \ldots. \alpha_n$, erit,

$$\log\Sigma \pm \frac{\partial x_1}{\partial \alpha_1} \cdot \frac{\partial x_2}{\partial \alpha_2} \ldots \frac{\partial x_n}{\partial \alpha_n} = \int\left(\frac{\partial X_1}{\partial x_1} + \frac{\partial X_2}{\partial x_2} \ldots + \frac{\partial X_n}{\partial x_n}\right) dx,$$

quantitate sub signo et ipsa per x et Constantes Arbitrarias expressa."

Si in Propositione antecedente ipsae $\alpha_1, \alpha_2, \ldots. \alpha_n$ designant variabilium valores initiales, valori $x = 0$ respondentes, integrationem inde a valore $x = 0$ fieri oportet. Ope huius Propositionis vel formulae generalioris (8.) fieri potest ut Quadratura alias satis abscondita eruatur; sicuti vice versa si Quadratura in promtu est, valor inde eruitur Determinantis functionalis.

Propositio antecedens primum a cl. *Liouville* tradita est in Commentatione *„sur la variation des constantes arbitraires,"* ipsius Diario Mathematico (Vol. III. pg. 342) inserta. Eadem sequitur e formula iam supra citata D. F. §. 9. (1.), loco f, f_1 etc. scribendo $x_1, x_2, \ldots. x_n$ atque x loco α, loco x_1, x_2 etc. autem $\alpha_1, \alpha_2, \ldots. \alpha_n$. Scilicet est ea consequentia lemmatis quod circa variationem logarithmi Determinantis loco citato dedi. Habeantur enim n systemata aequationum linearium inter n incognitas $u_1, u_2, \ldots. u_n$, quae systemata iisdem gaudeant Coëfficientibus incognitarum et tantum terminis prorsus constantibus inter se discrepent, unde etiam omnibus idem erit Determinans. Denotentur in $k$to aequationum linearium systemate termini constantes, in altera parte aequationum positi, respective per variationes Coëfficientium quibus in singulis aequationibus incognita u_k afficitur, atque e primo systemate aequationum petatur valor ipsius u_1, e secundo valor ipsius u_2, et ita porro: omnium horum valorum summa aequivalebit variationi logarithmi Determinantis.

In signis: sit $(u_k)_k$ valor ipsius u_k petitus e systemate aequationum,

$$10.\quad \begin{cases} a'_1 u_1 + a'_2 u_2 \dots + a'_n u_n = \delta a'_k, \\ a''_1 u_1 + a''_2 u_2 \dots + a''_n u_n = \delta a''_k, \\ \dots\dots\dots\dots\dots \\ a_1^{(n)} u_1 + a_2^{(n)} u_2 \dots + a_n^{(n)} u_n = \delta a_k^{(n)}, \end{cases}$$

erit

$$11.\quad (u_1)_1 + (u_2)_2 \dots + (u_n)_n = \delta \log \Sigma \pm a'_1 a''_2 \dots a_n^{(n)}.$$

Faciamus iam, in aequationibus differentialibus

$$\frac{dx_1}{dx} = X_1, \quad \frac{dx_2}{dx} = X_2, \quad \dots \quad \frac{dx_n}{dx} = X_n,$$

substitui variabilium $x_1, x_2, \dots x_n$ valores per x et Constantes Arbitrarias $\alpha_1, \alpha_2, \dots \alpha_n$ exhibitas, qua substitutione prodire debent aequationes identicae Quas si ipsarum α_i respectu differentiamus, obtinemus nn huiusmodi aequationes,

$$12.\quad d\frac{\partial x_k}{\partial \alpha_i} = \left\{ \frac{\partial X_k}{\partial x_1} \cdot \frac{\partial x_1}{\partial \alpha_i} + \frac{\partial X_k}{\partial x_2} \cdot \frac{\partial x_2}{\partial \alpha_i} \dots + \frac{\partial X_k}{\partial x_n} \cdot \frac{\partial x_n}{\partial \alpha_i} \right\} dx.$$

Ipsi i tribuendo valores $1, 2, \dots n$, ex aequatione antecedente prodeunt n aequationes lineares, in quibus habentur pro incognitis quantitates $\frac{\partial X_k}{\partial x_1} dx$, $\frac{\partial X_k}{\partial x_2} dx$ etc. Prodeunt n eiusmodi systemata aequationum linearum tribuendo ipsi quoque k valores $1, 2, \dots n$; in omnibusque illis aequationum linearium systematis incognitae iisdem gaudebunt Coëfficientibus. Hinc si in aequationibus (10.) ponimus

$$a_k^{(i)} = \frac{\partial x_k}{\partial \alpha_i},$$

atque variationibus substituimus differentialia, aequationes (10.) abeunt in aequationes (12.), unde eruitur

$$(u_k)_k = \frac{\partial X_k}{\partial x_k} dx.$$

Unde e (11.) sequitur

$$\left\{ \frac{\partial X_1}{\partial x_1} + \frac{\partial X_2}{\partial x_2} \dots + \frac{\partial X_n}{\partial x_n} \right\} dx = d \log \Sigma \pm \frac{\partial x_1}{\partial \alpha_1} \cdot \frac{\partial x_2}{\partial \alpha_2} \dots \frac{\partial x_n}{\partial \alpha_n}$$

qua formula integrata Propositio supra tradita obtinetur.

Aequationis $X - X_1 \frac{\partial x}{\partial x_1} - X_2 \frac{\partial x}{\partial x_2} \dots - X_n \frac{\partial x}{\partial x_n}$ pars laeva Multiplicatore suo efficitur Determinans functionale completum. Pro solutione singulari Multiplicator fit infinitus. Multiplicatorem nihilo aut infinito aequando obtinetur aequatio integralis.

§. 8.

Quemadmodum, proposito una plurium variabilium functione, destinguimus inter differentialia eius partialia, in quibus variabiles omnes pro independentibus habentur, et differentiale completum, in quo omnes ab earum una *indefinite* pendent, ita, propositis n functionibus $n+m$ variabilium, praeter earum Determinantia partialia, de quibus supra dixi, in quibus variabiles omnes pro independentibus habentur, in considerationem venire potest *Determinans completum*, quod formatur habendo numerum m variabilium pro reliquarum n functionibus *indefinitis*. Designantibus A et B ipsarum x et y functiones, aequationem differentialem,

$$A + B \frac{dy}{\partial x} = 0,$$

docuit *Eulerus*, semper in talem duci posse Multiplicatorem, ut altera aequationis pars evadat differentiale completum sive differentiale certae functionis variabilium x et y, in qua y pro functione ipsius x habetur *indefinita*. Similiter *aequatio differentialis partialis*,

$$1. \quad X - X_1 \frac{\partial x}{\partial x_1} - X_2 \frac{\partial x}{\partial x_2} \dots - X_n \frac{\partial x}{\partial x_n} = 0,$$

in qua X, X_1, ... X_n designant variabilium x, x_1, ... x_n functiones, semper in talem duci potest Multiplicatorem ut altera aequationis pars evadat Determinans functionale completum sive Determinans certarum n functionum variabilium x, x_1, x_2, ... x_n, in quibus habetur x pro variabilium x_1, x_2, ... x_n functione indefinita. Functio in aequationem (1.) ducenda ipse est aequationis (1.) *Multiplicator* supra appellatus et antecedentibus fusius explicatus. Unde nova nostri et *Euleriani* Multiplicatoris similitudo emergit novaque inter Determinantia functionalia et differentialia analogia.

Demonstratio Propositionis antecedentis sic patet. Designantibus rursus f_1, f_2, ... f_n solutiones a se independentes aequationis,

$$X \frac{\partial f}{\partial x} + X_1 \frac{\partial f}{\partial x_1} \dots + X_n \frac{\partial f}{\partial x_n} = 0,$$

supra vidimus, semper dari Multiplicatorem M, in quem ductae ipsae X, X_1, ... X_n evadant functionum f_1, f_2, ... f_n Determinantia partialia, ita ut po-

nendo pro functione f indefinita,

$$\Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n} = A\frac{\partial f}{\partial x} + A_1 \frac{\partial f}{\partial x_1} \cdots + A_n \frac{\partial f}{\partial x_n},$$

identice sit,

$$MX = A, \quad MX_1 = A_1, \quad \ldots \quad MX_n = A_n.$$

Hinc eruitur

$$2. \quad M\left\{X - X_1\frac{\partial x}{\partial x_1} - X_2\frac{\partial x}{\partial x_2} \cdots - X_n\frac{\partial x}{\partial x_n}\right\}$$
$$= A - A_1\frac{\partial x}{\partial x_1} - A_2\frac{\partial x}{\partial x_2} \cdots - A_n\frac{\partial x}{\partial x_n}.$$

At in Commentatione de Det. F. §. 17. (6.) demonstravi, siquidem in functionibus f_1, f_2, ... f_n habeatur x pro variabilium x_1, x_2, ... x_n functione indefinita, fieri,

$$3. \quad \Sigma \pm \left(\frac{\partial f_1}{\partial x_1}\right)\left(\frac{\partial f_2}{\partial x_2}\right) \cdots \left(\frac{\partial f_n}{\partial x_n}\right) = A - A_1\frac{\partial x}{\partial x_1} - A_2\frac{\partial x}{\partial x_2} \cdots - A_n\frac{\partial x}{\partial x_n}.$$

Qua in formula uncis innui haberi x pro reliquarum variabilium x_1, x_2, ... x_n functione. Scilicet in Determinante Functionali (3.) substituendo ipsorum $\left(\frac{\partial f_i}{\partial x_k}\right)$ expressiones

$$\left(\frac{\partial f_i}{\partial x_k}\right) = \frac{\partial f_i}{\partial x_k} + \frac{\partial f_i}{\partial x} \cdot \frac{\partial x}{\partial x_k},$$

mutuo destruuntur termini omnes, in quibus inter se multiplicata inveniuntur differentialia partialia $\frac{\partial x}{\partial x_1}$, $\frac{\partial x}{\partial x_2}$ etc., ita ut horum differentialium non nisi ipsa expressio *linearis* remaneat, quae dextram partem aequationis (3.) constituit. E (2.) et (3.) sequitur formula,

$$4. \quad M\left\{X - X_1\frac{\partial x}{\partial x_1} - X_2\frac{\partial x}{\partial x_2} \cdots - X_n\frac{\partial x}{\partial x_n}\right\}$$
$$= \Sigma \pm \left(\frac{\partial f_1}{\partial x_1}\right)\left(\frac{\partial f_2}{\partial x_2}\right) \cdots \left(\frac{\partial f_n}{\partial x_n}\right).$$

Unde ducta aequatione (1.) in Multiplicatorem eius M, altera eius pars identice aequatur Determinanti functionum f_1, f_2, ... f_n, in quibus x pro variabilium x_1, x_2, ... x_n functione habetur indefinita. Q. d. e.

Formula (4.) methodum suppeditat, ut *Lagrangii* appellatione utar, syntheticam ad eruendam aequationis (1.) solutionem generalem. Nam secundum (4.) aequatio (1.) identice convenit cum sequente,

$$5. \quad \Sigma \pm \left(\frac{\partial f_1}{\partial x_1}\right)\left(\frac{\partial f_2}{\partial x_2}\right) \cdots \left(\frac{\partial f_n}{\partial x_n}\right) = 0.$$

Quoties autem f_1, f_2, ... f_n sunt variabilium x_1, x_2, ... x_n functiones

earumque Determinans identice evanescit, semper et sine ulla exceptione inter functiones $f_1, f_2, \ldots f_n$ aliqua locum habere debet aequatio, et vice versa, si qua inter functiones $f_1, f_2, \ldots f_n$ locum habet aequatio, earum Determinans evanescit (D. F. §. 7.). Hinc docet formula (5.), ut ipsius x expressio per $x_1, x_2, \ldots x_n$ sit aequationis (1.) solutio, sufficere et posci, post eius substitutionem ipsas $f_1, f_2, \ldots f_n$ abire in tales variabilium $x_1, x_2, \ldots x_n$ functiones, inter quas una quaecunque locum habeat aequatio. Unde vice versa dabitur solutio generalis petendo functionis quaesitae valorem ex aequatione arbitraria inter $f_1, f_2, \ldots f_n$ posita,

$$\Pi(f_1, f_2, \ldots f_n) = 0;$$

sive quod idem est, obtinetur aequationis (1.) solutio nihilo aequando solutionem quamcunque aequationis,

$$6. \quad X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1} \ldots + X_n\frac{\partial f}{\partial x_n} = 0,$$

Haec egregia methodus aequationem differentialem partialem (1.) ad (6.) revocandi cum ea convenit quam olim ill. *Lagrange* tradidit (Hist. Ac. Ber. ad a. 1779 pag. 154), ubi primum hanc quaestionem aggressus est. Quae prolixior quidem videri possit methodus quam aliae quibus ipse *Lagrange* aliique postea usi sunt; qua de re ipse auctor eam ad exemplum tantum trium variabilium applicuit. Sane supponendo aequationem inter $x, x_1, \ldots x_n$ quaesitam certe unam involvere Constantem Arbitrariam α, eamque aequationem ipsius α respectu resolutam fieri $f = \alpha$, aequatio proposita (1.) extemplo ad (6.) reducitur. Sed eadem ratione omnes quoque inveniri solutiones a Constantibus Arbitrariis prorsus vacuas, non ita bene per alias methodos constat atque illam *Lagrangianam*. Scilicet aequatio identica (4.) docet, nullam dari exceptionem solutionis traditae, nisi forte exstet solutio pro qua Multiplicator M evadat infinitus. Quodsi igitur more consueto solutionem eiusmodi exceptionalem seu quae generali se subducit appellamus *singularem*, methodus hic tradita rigorose demonstrat, *si qua extet aequationis* (1.) *solutio singularis, semper eam reddere Multiplicatorem aequationis infinitum.* Quod novam nostri Multiplicatoris similitudinem cum *Euleriano* manifestat.

Loco aequationis differentialis partialis (1.) consideremus systema aequationum differentialium vulgarium cum ea connexum, atque systema aequationum integralium *singulare* appellemus quod e completo provenit tribuendo uni pluribusve Constantibus Arbitrariis valores particulares seu unam pluresve relationes inter Constantes Arbitrarias statuendo: quo facto ex antecedentibus haec eruitur

Propositio I.

„Proponantur aequationes differentiales

$$dx : dx_1 \ldots : dx_n = X : X_1 \ldots : X_n,$$

earumque extet systema aequationum integralium singulare, $n-1$ Constantes Arbitrarias involvens: eliminatis Constantibus Arbitrariis e n aequationibus integralibus, prodit aequatio quae Multiplicatorem systematis aequationum differentialium propositarum reddit infinitum."

Ut Propositio haec demonstretur, primum generaliter ponamus aequationes integrales datas $n-1$ Constantibus Arbitrariis affici. Quarum aequationum ubi $n-1$ resolvuntur Constantium Arbitrarium respectu, quod semper fieri posse suppono, harumque valores provenientes in $n$ta aequatione integrali substituuntur, obtinebitur aequatio a Constantibus Arbitrariis vacua. E qua petatur unius variabilium veluti x valor per reliquas variabiles x_1, x_2 etc. expressus, atque in differentiali eius,

$$dx = \frac{\partial x}{\partial x_1} dx_1 + \frac{\partial x}{\partial x_2} dx_2 \ldots + \frac{\partial x}{\partial x_n} dx_n,$$

substituantur aequationes differentiales propositae,

$$7. \quad dx : dx_1 \ldots : dx_n = X : X_1 \ldots : X_n;$$

eruitur

$$X = \frac{\partial x}{\partial x_1} X_1 + \frac{\partial x}{\partial x_2} X_2 \ldots + \frac{\partial x}{\partial x_n} X_n,$$

sive ille ipsius x valor suppeditabit aequationis differentialis partialis (1.) solutionem. Scilicet non fit ut aequatio antecedens ex aliis $n-1$ aequationibus integralibus datis fluat, quippe e quibus supponitur non deduci posse alteram aequationem a Constantibus Arbitrariis liberam. Eritque solutio illa aut particularis aut singularis, prout aequatio a Constantibus Arbitrariis libera, cuius ope ipsa x per reliquas variabiles exprimebatur, in aequationem inter quantitates f_1, f_2, ... f_n redit aut non redit. Iam demonstrabo, etiam systema aequationum integralium propositum iisdem casibus aut particulare aut singulare fore. Substituamus enim eum ipsius x valorem in $n-1$ aequationibus integralibus, quarum ope Constantes Arbitrariae eliminabantur, simulque in functionibus X_1, X_2, ... X_n aequationibus illis, ut $n-1$ Constantes Arbitrarias involventibus, *complete* integrantur aequationes differentiales

$$8. \quad dx_1 : dx_2 \ldots : dx_n = X_1 : X_2 \ldots : X_n.$$

Unde quibuscunque aequationibus integralibus, $n-1$ Constantes Arbitrarias involventibus, semper haec forma conciliari potest, ut earum una exhibeatur una variabilium x per reliquas variabiles x_1, x_2, etc., reliquae $n-1$ aequationes

autem sint Integralia completa aequationum differentialium (8.), in quibus ille ipsius x valor in functionibus X_1, X_2, ... X_n substitutus est. Ponamus aequationem illam a Constantibus Arbitrariis vacuam, e qua valor ipsius x petitus est, redire in aequationem aliquam $F=0$, designante F quantitatum $f_1, f_2, \ldots f_n$ functionem. Designantibus $F, F_1, \ldots . F_{n-1}$ earundem $f_1, f_2, \ldots . f_n$ functiones a se invicem independentes, dabitur aequationum differentialium propositarum (7.) integratio completa per formulas

$$9. \quad F=\alpha, \quad F_1=\alpha_1, \quad \ldots . \quad F_{n-1}=\alpha_{n-1},$$

designantibus α, α_1 etc. Constantes Arbitrarias. Ex aequatione $F=\alpha$ petito ipsius x valore eoque in functionibus $F_1, F_2, \ldots . F_{n-1}, X_1, X_2, \ldots . X_n$ substituto, evadunt

$$F_1=\alpha_1, \quad F_2=\alpha_2, \ldots . F_{n-1}=\alpha_{n-1}$$

Integralia completa aequationum differentialium,

$$dx_1 : dx_1 \ldots . : dx_n = X_1 : X_2 \ldots . : X_n,$$

quae cum aequationibus differentialibus (8.) supra consideratis conveniunt ponendo $\alpha=0$. Unde ponendo $\alpha=0$ in aequationum differentialium propositarum Integralibus completis (9.), prodit systema aequationum integralium propositarum. Quippe quae redibant in aequationem qua ipsa x exprimitur per reliquas variabiles et quae cum aequatione $F=0$ conveniebat, atque in aequationum differentialium (8.) Integralia completa, quae ex aequationibus $F_1=\alpha_1$, $F_2=\alpha_2$, ... $F_{n-1}=\alpha_{n-1}$ obtinentur, eliminata x ope aequationis $F=0$. Unde aequationibus differentialibus (7.) integratis systemate aequationum, $n-1$ Constantes Arbitrarias involventium, quoties aequatio eliminatione Constantium Arbitrariarum proveniens redit in aequationem inter ipsas $f_1, f_2, \ldots . f_n$, illud aequationum integralium systema erit particulare, utpote e completo proveniens tribuendo Constanti Arbitrariae valorem particularem. Hinc vice versa, si illud aequationum integralium systema non est particulare, aequatio eliminatione $n-1$ Constantium Arbitrariarum proveniens non redit in aequationem inter quantitates $f_1, f_2, \ldots . f_n$, ideoque solutio quam suppeditat aequationis differentialis partialis (1.) erit singularis. Cuiusmodi solutione, cum secundum antecedentibus probata efficiatur $M=\infty$, demonstratum est quod propositum erat, *quoties systema aequationum differentialium vulgarium integretur systemate aequationum singulari, numerum Constantium Arbitrariarum involvente unitate minorem quam completum involvit, Constantium Arbitrariarum eliminatione provenire aequationem, qua Multiplicator systematis aequationum differentialium abeat in infinitum.* Et in hac propositione supponitur, quantitates X, X_1 etc. ita a

denominatoribus purgatas esse, ut earum nulla pro illa aequatione integrali seu solutione singulari infinita evadat.

Propositionis antecedentis alia haec est demonstratio. Integratione completa exprimantur x_1, x_2, ... x_n per x et Constantes Arbitrarias β_1, β_2, ... β_n. Ponamus aequationibus differentialibus satisfieri posse statuendo β_1, β_2, ... β_n esse ipsius x functiones; sequitur e formula,

$$dx_i = \frac{\partial x_i}{\partial x}dx + \frac{\partial x_i}{\partial \beta_1}d\beta_1 + \frac{\partial x_i}{\partial \beta_2}d\beta_2 \ldots + \frac{\partial x_i}{\partial \beta_n}d\beta_n,$$

haec

$$\frac{X_i}{X}dx = \frac{\partial x_i}{\partial x}dx + \frac{\partial x_i}{\partial \beta_1}d\beta_1 + \frac{\partial x_i}{\partial \beta_2}d\beta_2 \ldots + \frac{\partial x_i}{\partial \beta_n}d\beta_n$$

At eliminando quantitates β_1, β_2, ... β_n sequitur ex aequationibus integralibus positis,

$$\frac{X_i}{X} = \frac{\partial x_i}{\partial x},$$

quippe quod prodire debebat ponendo β_1, β_2, ... β_n esse Constantes; illis autem eliminatis quantitatibus perinde est sive constantes sive variabiles fuerint. Substituendo aequationem antecedentem eruitur pro singulis ipsius i valoribus,

$$10.\quad \frac{\partial x_i}{\partial \beta_1}d\beta_1 + \frac{\partial x_i}{\partial \beta_2}d\beta_2 \ldots + \frac{\partial x_i}{\partial \beta_n}d\beta_n = 0.$$

Ut satisfiat n aequationibus quae ponendo $i = 1, 2, \ldots n$ ex antecedente fluunt, neque simul sit $d\beta_1 = d\beta_2 \ldots = d\beta_n = 0$ sive β_1, β_2, ... β_n Constantes sint, evadere debet

$$11.\quad \Sigma \pm \frac{\partial x_1}{\partial \beta_1} \cdot \frac{\partial x_2}{\partial \beta_2} \ldots \frac{\partial x_n}{\partial \beta_n} = 0.$$

Quoties poscitur ut functiones β_1, β_2, ... β_n involvant $n-1$ Constantes Arbitrarias, non fieri potest ut aequatio (11.) in relationem inter solas variabiles β_1, β_2, ... β_n redeat, sed fieri debet ut e (11.) peti possit ipsius x valor per β_1, β_2, ... β_n expressus; quo substituto in quantitatibus $\frac{\partial x_i}{\partial \beta_k}$, habebuntur e (10.) $n-1$ aequationes differentiales primi ordinis inter quantitates β_1, β_2, ... β_n, quibus complete integratis prodibunt $n-1$ aequationes inter quantitates β_1, β_2, ... β_n, $n-1$ Constantibus Arbitrariis affectae. Quibus $n-1$ aequationibus iuncta aequatione qua x per β_1, β_2, ... β_n exprimebatur, ipsarumque β_1, β_2 etc. loco substitutis variabilium x, x_1, ... x_n functionibus, quibus per integrationem completam aequivalent, obtinetur systema aequationum integralium singularium, $n-1$ Constantibus Arbitrariis affectum. Fit autem se-

cundum §. 6.,

$$\Sigma \pm \frac{\partial x_1}{\partial \beta_1} \cdot \frac{\partial x_2}{\partial \beta_2} \cdots \frac{\partial x_n}{\partial \beta_n} = \frac{C}{X_\mu},$$

designante C quantitatum $\beta_1, \beta_2, \ldots \beta_n$ functionem atque μ aequationum differentialium propositarum Multiplicatorem. Unde, cum supponatur aequationem (10.) non redire in relationem inter quantitates $\beta_1, \beta_2, \ldots \beta_n$, porro ipsam X non infinitam evadere, sequitur e (10.) $\mu = \infty$, q. d. e.

Secundum ea quae §. 7. tradidi, Multiplicator M systematis aequationum differentialium post earum integrationem completam factam sic erui potest. Sint rursus Integralia completa,

$$f_1 = \alpha_1, \quad f_2 = \alpha_2, \quad \ldots \quad f_n = \alpha_n,$$

eorum ope exprimatur

$$-\frac{1}{X}\left\{\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \cdots + \frac{\partial X_n}{\partial x_n}\right\}$$

per $x, \alpha_1, \alpha_2, \ldots \alpha_n$. Qua expressione integrata ipsius x respectu, prodeat

$$\varphi(x, \alpha_1, \alpha_2, \ldots \alpha_n),$$

secundum §. 7. erit Multiplicator

$$e^{\varphi(x, f_1, f_2, \ldots f_n)}.$$

Haec quantitas ut infinita evadat per solutionem seu aequationem integralem singularem, hoc est per solutionem seu aequationem integralem quae non redeat in aequationem inter solas quantitates $f_1, f_2, \ldots f_n$ (quod semper fieri vidimus quoties omnino eiusmodi aequatio singularis extat) ex ea aequatione talis provenire debet valor ipsius x per quantitates $f_1, f_2, \ldots f_n$ expressus, quae quantitatem $\varphi(x, f_1, f_2, \ldots f_n)$ reddat infinitam. A *fortiori* igitur pro ea ipsius x valore infinita evadere debet quantitas

$$\frac{\partial \varphi}{\partial x} = -\frac{1}{X}\left\{\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \cdots + \frac{\partial X_n}{\partial x_n}\right\},$$

cum generaliter *quoties pro certo ipsius x valore infinita evadat functio aliqua $\varphi(x)$, pro eadem etiam infinita evadit functio $\frac{\partial \varphi}{\partial x}$ vel adeo $\frac{\partial \varphi}{\varphi \partial x}$* *). Supponimus autem, aequatione singulari non in infinitum abire quantitatem X, unde haec emergit

Propositio II.

„*Quoties extat solutio singularis aequationis differentialis partialis,*

$$X = X_1 \frac{\partial x}{\partial x_1} + X_2 \frac{\partial x}{\partial x_2} \cdots + X_n \frac{\partial x}{\partial x_n},$$

*) Demonstrationem huius propositionis quivis sibi supplere potest.

pro eadem fit

$$\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\cdots\cdot+\frac{\partial X_n}{\partial x_n}=\infty."$$

Difficilius videtur solidis argumentis evincere propositionem inversam, videlicet quoties aequatio

$$\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\cdots\cdot+\frac{\partial X_n}{\partial x_n}=\infty$$

suppeditet aequationis differentialis partialis (1.) solutionem, eam fore singularem. Neque video solidam dari demonstrationem in casu elementari aequationis differentialis primi ordinis inter duas variabiles, cum in demonstrationibus passim traditis minus recte supponatur, functionem quae pro $\alpha=0$ evanescat semper evolvi posse secundum ipsius α dignitates positivas.

Sub finem demonstretur de Multiplicatore nostro haec gravissima

Propositio III.

„*Quoties aequatio $M=0$ aut $M=\infty$ est aequatio legitima, semper ea suppeditat solutionem aequationis differentialis partialis, seu aequationem integralem systematis aequationum differentialium vulgarium, cuius M est Multiplicator.*"

Sit M aut $\frac{1}{M}$ aequale functioni u, ita ut aequatio $u=\infty$ alterutram significet aequationum $M=0$ aut $\frac{1}{M}=0$. Eam aequationem legitimam dico si eius ope quaeque variabilium quas continet determinatur ut functio reliquarum, eiusque differentialia quoque prorsus definiantur differentialibus reliquarum variabilium. Statim patet non esse legitimam aequationem $u=\infty$, si est $u=1$; sed eo dicendi modo etiam non erit legitima huiusmodi aequatio $\frac{1}{x+y}=0$, quippe qua non definitur, ut ipsius x functio, sed enunciatur tantum $x+y$ esse functionem quamcunque per Constantem infinite magnam multiplicatam; neque definitur ipsius y incrementum quod capit, ubi x in $x+dx$ abit, cum aequatio $x+y=\infty$ salva maneat si x et y incrementa quaecunque a se independentia capiunt. Addo, si ex aequatione $u=\infty$ fluat variabilis x valor per $x_1, x_2, \ldots. x_n$ expressus, fractiones $\frac{\partial u}{\partial x_i}:\frac{\partial u}{\partial x}$ per aequationem $u=\infty$ infinitas evadere non posse, cum negative sumtae aequentur differentialibus partialibus functionis variabilium $x_1, x_2, \ldots. x_n$, cui x aequalis invenitur. His praeparatis propositio tradita sic patet. Secundum aequationem differentialem partialem qua M defi-



nitur, sequitur ex aequatione $u = \infty$,

$$12. \quad X - X_1 \frac{\partial x}{\partial x_1} - X_2 \frac{\partial x}{\partial x_2} \dots - X_n \frac{\partial x}{\partial x_n}.$$
$$= \pm \frac{1}{\frac{\partial \log u}{\partial x}} \left\{ \frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \dots + \frac{\partial X_n}{\partial x_n} \right\}.$$

Iam si supponitur, uti supra, aequatione $u = \infty$ nullam quantitatem $X, X_1, \dots X_n$ infinitam reddi, quaelibet quantitatum ad dextram, $\frac{\partial X_i}{\partial x_i} : \frac{\partial \log u}{\partial x}$, pro $u = \infty$ evanescit, etsi $\frac{\partial X_i}{\partial x_i}$ pro $u = \infty$ infinitum fiat. Quod sufficit probare de quantitate $\frac{\partial X_i}{\partial x_i} : \frac{\partial \log u}{\partial x_i}$, cum fractio $\frac{\partial u}{\partial x_i} : \frac{\partial u}{\partial x}$ valorem finitum habeat. Generale autem habetur lemma cuius demonstrationi difficultatibus non obnoxiae hic brevitatis causa supersedeo, *si binae functiones pro certo variabilis valore altera infinita fiat, altera finita maneat, prioris differentiale pro eodem variabilis valore infinite maius fore quam posterioris differentiale.* Petendo autem ex aequatione $u = \infty$ valorem ipsius x_i, pro eo ipsius x_i valore secundum suppositionem factam X_i finita manet dum $\log u$ infinitus evadit, unde fractiones $\frac{\partial X_i}{\partial x_i} : \frac{\partial \log u}{\partial x_i}$ ideoque etiam fractiones $\frac{\partial X_i}{\partial x_i} : \frac{\partial \log u}{\partial x}$ pro $u = \infty$ evanescunt. Unde evanescente aequationis (12.) parte dextra, aequatio $u = \infty$ suppeditat aequationis differentialis partialis (1.) solutionem, ideoque etiam aequationem integralem systematis aequationum differentialium vulgarium (7.)

Notione aequationis legitimae supra propositae solvitur paradoxon quod in theória integrationum singularium obvenit. Constat enim rarissime aequationes differentiales gaudere integrationibus singularibus. At methodus *Lagrangiana* quandam prae se fert generalitatis speciem, quae in errorem inducere possit, ac si de quavis integratione completa deducere liceat singularem. Scilicet ill. *Lagrange,* de aequationibus $y = f(x, \alpha)$, $\frac{\partial f}{\partial \alpha} = 0$, ipsum α eliminare iubet; at in rarissimis casibus quando $y = f(x, \alpha)$ est aequatio integralis completa, Constante Arbitraria α affecta, fit $\frac{\partial f}{\partial \alpha} = 0$ aequatio legitima, qua sola hic uti licet. Idem ad methodum valet, qua supra de systemate aequationum integralium completarum deduxi aequationum integralium singularium systema, quod numerum Constantium Arbitrariarum unitate minorem implicat.

Caput secundum.

De usu novi Multiplicatoris in aequationibus differentialibus integrandis. Principium ultimi Multiplicatoris.

De Multiplicatore aequationum differentialium transformatarum e propositarum derivando.

§. 9.

In aequationibus differentialibus propositis,

$$1. \quad dx : dx_1 \dots : dx_n = X : X_1 \dots : X_n,$$

loco variabilium $x, x_1, \dots x_n$ aliae introducantur $w, w_1, \dots w_n$, quae supponuntur datae variabilium $x, x_1, \dots x_n$ functiones a se independentes, unde etiam $x, x_1, \dots x_n$ erunt quantitatum $w, w_1, \dots w_n$ functiones independentes. Cum fiat,

$$dw_i = \frac{\partial w_i}{\partial x} dx + \frac{\partial w_i}{\partial x_1} dx_1 \dots + \frac{\partial w_i}{\partial x_n} dx_n,$$

sequitur ex aequationibus (1.):

$$2. \quad dw : dw_1 \dots : dw_n = W : W_1 \dots : W_n,$$

ponendo,

$$3. \quad W_i = \Delta \left\{ \frac{\partial w_i}{\partial x} X + \frac{\partial w_i}{\partial x_1} X_1 \dots + \frac{\partial w_i}{\partial x_n} X_n \right\},$$

ubi Δ factor adhuc indeterminatus sit. Porro fit,

$$\frac{\partial f}{\partial x_i} = \left(\frac{\partial f}{\partial w}\right) \frac{\partial w}{\partial x_i} + \left(\frac{\partial f}{\partial w_1}\right) \frac{\partial w_1}{\partial x_i} \dots + \left(\frac{\partial f}{\partial w_n}\right) \frac{\partial w_n}{\partial x_i},$$

siquidem uncis, quibus includimus differentialia partialia, innuimus functiones differentiandas per novas variabiles $w, w_1, \dots w_n$ exhibitas esse. Antecedente formula substituta et advocata (3.) sequitur *pro quacunque functione f:*

$$4. \quad \Delta \left\{ X \frac{\partial f}{\partial x} + X_1 \frac{\partial f}{\partial x_1} \dots + X_n \frac{\partial f}{\partial x_n} \right\}$$
$$= W \left(\frac{\partial f}{\partial w}\right) + W_1 \left(\frac{\partial f}{\partial w_1}\right) \dots + W_n \left(\frac{\partial f}{\partial w_n}\right).$$

Aequationum (1.) Multiplicator M definiebatur aequatione,

$$5. \quad M \left\{ X \frac{\partial f}{\partial x} + X_1 \frac{\partial f}{\partial x_1} \dots + X_n \frac{\partial f}{\partial x_n} \right\} = \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \dots \frac{\partial f_n}{\partial x_n}.$$

Similiter datur aequationum (2.) Multiplicator N per formulam,

$$6. \quad N \left\{ W \left(\frac{\partial f}{\partial w}\right) + W_1 \left(\frac{\partial f}{\partial w_1}\right) \dots + W_n \left(\frac{\partial f}{\partial w_n}\right) \right\}$$
$$= \Sigma \pm \left(\frac{\partial f}{\partial w}\right) \left(\frac{\partial f_1}{\partial w_1}\right) \dots \left(\frac{\partial f_n}{\partial w_n}\right).$$

At secundum propositionem notam (*De Determ. Funct.* §. 11. *Prop.* II. §. 9. (3.)) fit,

$$7. \quad \Sigma \pm \frac{\partial f}{\partial x} \cdot \frac{\partial f_1}{\partial x_1} \cdots \frac{\partial f_n}{\partial x_n}$$
$$= \Sigma \pm \left(\frac{\partial f}{\partial w}\right)\left(\frac{\partial f_1}{\partial w_1}\right) \cdots \left(\frac{\partial f_n}{\partial w_n}\right) \cdot \Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots \frac{\partial w_n}{\partial x_n}.$$

Unde e (4.), (5.) obtinetur pro quacunque functione f:

$$8. \quad \frac{M}{\varDelta}\left\{W\left(\frac{\partial f}{\partial w}\right) + W_1\left(\frac{\partial f_1}{\partial w_1}\right) \cdots + W_n\left(\frac{\partial f_n}{\partial w_n}\right)\right\}$$
$$= \Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots \frac{\partial w_n}{\partial x_n} \cdot \Sigma \pm \left(\frac{\partial f}{\partial w}\right)\left(\frac{\partial f_1}{\partial w_1}\right) \cdots \left(\frac{\partial f_n}{\partial w_n}\right).$$

Quam formulam comparando cum (6.) sequitur, *posito in formula* (3.),

$$9. \quad \varDelta = \frac{1}{\Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots \frac{\partial w_n}{\partial x_n}} = \Sigma \pm \left(\frac{\partial x}{\partial w}\right)\left(\frac{\partial x_1}{\partial w_1}\right) \cdots \left(\frac{\partial x_n}{\partial w_n}\right),$$

fieri $N = M$ *sive aequationum differentialium propositarum* (1.) *atque transformatarum* (2.) *eundem fore Multiplicatorem.*

Servando factori $\varDelta$ valorem (9.), cum sit idem M aequationum (1.) et (2) Multiplicator, fit e proprietate Multiplicatoris fundamentali,

$$10. \quad 0 = X\frac{\partial M}{\partial x} + X_1\frac{\partial M}{\partial x_1} \cdots + X_n\frac{\partial M}{\partial x_n}$$
$$+ M\left\{\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \cdots + \frac{\partial X_n}{\partial x_n}\right\},$$

$$11. \quad 0 = W\left(\frac{\partial M}{\partial w}\right) + W_1\left(\frac{\partial M}{\partial w_1}\right) \cdots + W_n\left(\frac{\partial M}{\partial w_n}\right)$$
$$+ M\left\{\left(\frac{\partial W}{\partial w}\right) + \left(\frac{\partial W_1}{\partial w_1}\right) \cdots + \left(\frac{\partial W_n}{\partial w_n}\right)\right\}.$$

At ponendo M pro functione indefinita f in formula (4.) fit,

$$X\frac{\partial M}{\partial x} + X_1\frac{\partial M}{\partial x_1} \cdots + X_n\frac{\partial M}{\partial x_n} = \frac{1}{\varDelta}\left\{W\frac{\partial M}{\partial w} + W_1\frac{\partial M}{\partial w_1} \cdots + W_n\frac{\partial M}{\partial w_n}\right\}.$$

Unde de aequatione (11.) per $\varDelta$ divisa detrahendo aequationem (10.) et dividendo per M eruitur:

$$12. \quad \frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \cdots + \frac{\partial X_n}{\partial x_n} = \frac{1}{\varDelta}\left\{\left(\frac{\partial W}{\partial w}\right) + \left(\frac{\partial W_1}{\partial w_1}\right) \cdots + \left(\frac{\partial W_n}{\partial w_n}\right)\right\}.$$

Quae est formula memoratu digna, in qua $X, X_1, \ldots X_n$ sunt functiones quaecunque, ipsae autem $\varDelta$, W, $W_1, \ldots W_n$ formulis (9.) et (3.) definiuntur.

Si quantitates W, W_1 etc. per factorem communem $\varDelta$ dividimus, per eundem multiplicandus erit aequationum (2.) Multiplicator. Unde si definimus

quantitates W_i formula

$$W_i = \frac{\partial w_i}{\partial x} X + \frac{\partial w_i}{\partial x_1} X_1 \dots + \frac{\partial w_i}{\partial x_n} X_n,$$

aequationum differentialium,

$$dw : dw_1 \dots dw_n = W : W_1 \dots : W_n,$$

erit Multiplicator $\Delta.M.$ Ponamus

$$t = \int \frac{dx}{X},$$

poterunt aequationes differentiales (1.) sic proponi:

$$13.\quad \frac{dx}{dt} = X,\quad \frac{dx_1}{dt} = X_1,\quad \dots \quad \frac{dx_n}{dt} = X_n;$$

unde sequitur,

$$\frac{dw_i}{dt} = \frac{\partial w_i}{\partial x} X + \frac{\partial w_i}{\partial x_1} X_1 \dots + \frac{\partial w_i}{\partial x_n} X_n,$$

sive,

$$\frac{dw_i}{dt} = W_i.$$

***Aequationum* (1.) *Multiplicatorem in sequentibus etiam appellabo Multiplicatorem aequationum* (13.).** Unde antecedentibus inventa sic poterunt enunciari:

Propositio I.

„Designantibus $X, X_1, \dots X_n$ variabilium $x, x_1, \dots x_n$ functiones quaslibet, proponantur aequationes differentiales,

$$\frac{dx}{dt} = X,\quad \frac{dx_1}{dt} = X_1,\quad \dots \quad \frac{dx_n}{dt} = X_n,$$

quarum sit M Multiplicator; in quibus aequationibus ipsarum x, x_1 etc. loco aliae introducantur variabiles $w, w_1, \dots w_n$; quo facto si obtinentur aequationes differentiales,

$$14.\quad \frac{dw}{dt} = W,\quad \frac{dw_1}{dt} = W_1,\quad \dots \quad \frac{dw_n}{dt} = W_n,$$

harum aequationum Multiplicator erit $\Delta.M$, posito

$$\Delta = \frac{1}{\Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \dots \frac{\partial w_n}{\partial x_n}} = \Sigma \pm \left(\frac{\partial x}{\partial w}\right) \left(\frac{\partial x_1}{\partial w_1}\right) \dots \left(\frac{\partial x_n}{\partial w_n}\right)."$$

Ubi rursus quantitates W_i formula (3.) definimus, formulam (12.) sic proponere licet.

Propositio II.

„Ipsarum x, x_1, ... x_n loco introducendo w, w_1, ... w_n, ponendoque

$$d t = \Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots \frac{\partial w_n}{\partial x_n} \cdot d t,$$

ex aequationibus differentialibus

$$\frac{dx}{dt} = X, \quad \frac{dx_1}{dt} = X_1, \quad \dots \quad \frac{dx_n}{dt} = X_n,$$

proveniant sequentes,

$$\frac{dw}{dt} = W, \quad \frac{dw_1}{dt} = W_1, \quad \dots \quad \frac{dw_n}{dt} = W_n,$$

erit

$$\left\{\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \dots + \frac{\partial X_n}{\partial x_n}\right\} dt = \left\{\left(\frac{\partial W}{\partial w}\right) + \left(\frac{\partial W_1}{\partial w_1}\right) \dots + \left(\frac{\partial W_n}{\partial w_n}\right)\right\} dt."$$

In antecedentibus suppositum est, neque ipsas X, X_1 etc. implicare variabilem t neque eam variabilem afficere relationes quae inter variabiles propositas x, x_1, ... x_n atque novas w, w_1, ... w_n intercedunt. *Si quantitates X, X_1 etc. praeter variabiles x, x_1 etc. ipsa quoque t afficiuntur, aequationum* (13.) *Multiplicatorem eundem dicere placet atque aequationum,*

$$15. \quad dt : dx : dx_1 \dots . dx_n = 1 : X : X_1 \dots . : X_n.$$

Designantibus x, x_1 etc. ipsarum t, w, w_1, ... w_n, sive w, w_1 etc. ipsarum t, x, x_1, ... x_n functiones, ponamus rursus ex aequationibus differentialibus (13.) vel (15.) sequi aequationes (14.) sive aequationes,

$$16. \quad dt : dw : dw_1 \dots . dw_n = 1 : W : W_1 \dots . : W_n,$$

atque aequationum (15.) Multiplicatorem esse M, aequationum (16.) Multiplicatorem $\Delta . M$. Quibus statutis, secundum antecedentia ad $n+2$ variabiles amplificata erit,

$$\Delta = \Sigma \pm \left(\frac{\partial t}{\partial t}\right)\left(\frac{\partial x}{\partial w}\right)\left(\frac{\partial x_1}{\partial w_1}\right) \dots \left(\frac{\partial x_n}{\partial w_n}\right).$$

Sed habetur $\left(\frac{\partial t}{\partial t}\right) = 1$, $\left(\frac{\partial t}{\partial w_i}\right) = 0$, unde,

$$\Sigma \pm \left(\frac{\partial t}{\partial t}\right)\left(\frac{\partial x}{\partial w}\right)\left(\frac{\partial x_1}{\partial w_1}\right) \dots \left(\frac{\partial x_n}{\partial w_n}\right) = \Sigma \pm \left(\frac{\partial x}{\partial w}\right)\left(\frac{\partial x_1}{\partial w_1}\right) \dots \left(\frac{\partial x_n}{\partial w_n}\right).$$

Hinc sequitur, *Propositionem I. ad eum quoque casum valere, quo quantitates X, X_1 etc. atque functiones novis variabilibus aequandae w, w_1 etc. praeter ipsas x, x_1 etc. variabili t afficiuntur.*

Si tantum pro parte variabilium aliae introducuntur, ipsius Δ expressio simplicior evadit. Propositis enim aequationibus (13.)

$$\frac{dx}{dt} = X, \quad \frac{dx_1}{dt} = X_1, \quad \ldots\ldots \quad \frac{dx_n}{dt} = X_n,$$

quarum est M Multiplicator, si tantum loco variabilium $x, x_1, \ldots\ldots x_\mu$ aliae introducuntur $w, w_1, \ldots\ldots w_\mu$, ita ut aequationes differentiales transformatae fiant,

$$\frac{dw}{dt} = W, \quad \frac{dw_1}{dt} = W_1, \quad \ldots\ldots \quad \frac{dw_\mu}{dt} = W_\mu,$$

$$\frac{dx_{\mu+1}}{dt} = X_{\mu+1}, \quad \frac{dx_{\mu+2}}{dt} = X_{\mu+2}, \quad \ldots\ldots \quad \frac{dx_n}{dt} = X_n,$$

fit harum Multiplicator $\Delta . M$, posito,

$$\Delta = \Sigma \pm \left(\frac{\partial x}{\partial w}\right)\left(\frac{\partial x_1}{\partial w_1}\right) \ldots\ldots \left(\frac{\partial x_\mu}{\partial w_\mu}\right) = \frac{1}{\Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots\cdots \frac{\partial w_\mu}{\partial x_\mu}},$$

sicuti ex expressione generali ipsius Δ patet ponendo $w_{\mu+1} = x_{\mu+1}$, $w_{\mu+2} = x_{\mu+2}$ etc. Quae formulae variis applicationibus idoneae sunt.

Multiplicator aequationum differentialium ope Integralium completorum reductarum e Multiplicatore propositarum eruitur. Pro reductionibus diversis Multiplicatores alii de aliis deducuntur.

§. 10.

Per formulas §. pr. traditas facile solvitur quaestio, si aequationum differentialium

$$1. \quad dx : dx_1 \ldots\ldots : dx_n = X : X_1 \ldots\ldots : X_n,$$

inventa sint m Integralia,

$$2. \quad w = \alpha, \quad w_1 = \alpha_1, \quad \ldots\ldots \quad w_{m-1} = \alpha_{m-1},$$

designantibus $\alpha, \alpha_1, \ldots\ldots \alpha_{m-1}$ Constantes Arbitrarias, aequationum differentialium ope illorum Integralium reductarum Multiplicatorem e Multiplicatore propositarum investigandi. Sint enim $w_m, w_{m+1}, \ldots\ldots w_n$ aliae variabilium $x, x_1, \ldots\ldots x_n$ functiones a se ipsis et ab ipsis $w, w_1, \ldots\ldots w_{m-1}$ independentes, inter quas propositum sit aequationes differentiales exhibere reductas. Poterunt $w, w_1, \ldots\ldots w_n$ ipsarum $x, x_1, \ldots\ldots x_n$ loco pro variabilibus in Calculum introduci. Quo facto secundum §. pr. abeunt aequationes differentiales vulgares (1.) in sequentes:

$$3. \quad dw : dw_1 : dw_2 \ldots\ldots : dw_n = W : W_1 : W_2 \ldots\ldots : W_n,$$

siquidem statuitur

$$4. \quad W_i = \Delta \left\{ \frac{\partial w_i}{\partial x} + X_1 \frac{\partial w_i}{\partial x_1} \ldots\ldots + X_n \frac{\partial w_i}{\partial x_n} \right\}.$$

Ponendo factorem Δ, quem ex arbitrio determinare licet, fieri,

$$5.\quad \Delta = \Sigma \pm \left(\frac{\partial x}{\partial w}\right)\left(\frac{\partial x_1}{\partial w_1}\right)\cdots\left(\frac{\partial x_n}{\partial w_n}\right) = \frac{1}{\Sigma \pm \frac{\partial w}{\partial x}\cdot\frac{\partial w_1}{\partial x_1}\cdots\frac{\partial w_n}{\partial x_n}},$$

vidimus §. pr. Multiplicatorem aequationum differentialium propositarum (1.) eundem evadere Multiplicatorem aequationum transformatarum (3.). Unde designante M aequationum (1.) Multiplicatorem, identice erit

$$6.\quad \left(\frac{\partial . MW}{\partial w}\right) + \left(\frac{\partial . MW_1}{\partial w_1}\right)\cdots + \left(\frac{\partial . MW_n}{\partial w_n}\right) = 0,$$

qua in formula M, W, W_1, ... W_n per variabiles w, w_1, ... w_n expressae finguntur. At cum sint (2.) aequationum differentialium (1.) Integralia, sequitur esse w, w_1, ... w_{m-1} solutiones aequationis differentialis partialis

$$X\frac{\partial f}{\partial x} + X_1\frac{\partial f}{\partial x_1}\cdots + X_n\frac{\partial f}{\partial x_n} = 0,$$

unde patet e formula (4.), identice fieri,

$$7.\quad W = 0,\quad W_1 = 0,\quad \ldots\quad W_{m-1} = 0.$$

Unde aequatio (6.) in hanc reducitur,

$$8.\quad \left(\frac{\partial . MW_m}{\partial w_m}\right) + \left(\frac{\partial . MW_{m+1}}{\partial w_{m+1}}\right)\cdots + \left(\frac{\partial . MW_n}{\partial w_n}\right) = 0.$$

In aequatione antecedente expressae sunt MW_m, MW_{m+1} etc. per w, w_1, ... w_n, sed differentiationes partiales solarum w_m, w_{m+1}, ... w_n respectu transiguntur. Unde in aequatione praecedente ipsis w, w_1, ... w_{m-1} substituere licet Constantes Arbitrarias aequivalentes α, α_1, ... α_{m-1}. Idem si facimus in aequationibus differentialibus (3.), obtinemus aequationes differentiales per inventa Integralia (2.) reductas,

$$9.\quad dw_m : dw_{m+1} \ldots : dw_n = W_m : W_{m+1} \ldots : W_n,$$

in quibus sunt W_m, W_{m+1}, ... W_n ipsarum w_m, w_{m+1}, ... w_n et Constantium Arbitrariarum α, α_1, ... α_{m-1} functiones, in quas quantitates (4.) per inventa Integralia (2.) abeunt. Simulque docet aequatio identica (8.) ipsum M, per w_m, w_{m+1}, ... w_n atque α, α_1, ... α_{m-1} expressum, fore aequationum quoque reductarum (9.) Multiplicatorem.

Antecedentibus valores quantitatum W_i per talem factorem Δ multiplicavi, ut aequationum differentialium (1.) atque (3.) Multiplicator M idem fiat. Si in formulis (4.) hunc factorem omittimus sive omnes quantitates W_i per factorem Δ dividimus, ipsum M per eundem multiplicari debebat, sive aequationum (3.) vel (9.) Multiplicator poni debebat $\Delta . M$ (§. 9.). Quod si facimus, antecedentibus inventa sic proponere licet.

Propositio I.

„Aequationum differentialium

$$dx : dx_1 \dots : dx_n = X : X_1 \dots : X_n,$$

quarum sit M Multiplicator, inventa sint m Integralia,

$$w = \alpha, \quad w_1 = \alpha_1, \quad \dots \quad w_{m-1} = \alpha_{m-1},$$

quorum ope variabiles $x, x_1, \dots x_n$ omnes exprimantur per Constantes Arbitrarias $\alpha, \alpha_1, \dots \alpha_{m-1}$ atque variabilium $x, x_1, \dots x_n$ functiones

$$w_m, \quad w_{m+1}, \quad \dots \quad w_n,$$

ponendo

$$W_i = X\frac{\partial w_i}{\partial x} + X_1\frac{\partial w_i}{\partial x_1} \dots + X_n\frac{\partial w_i}{\partial x_n},$$

dabuntur inter variabiles $w_m, w_{m+1}, \dots w_n$ aequationes differentiales,

$$dw_m : dw_{m+1} \dots : dw_n = W_m : W_{m+1} \dots : W_n,$$

harumque Multiplicator erit

$$\Delta . M,$$

siquidem ponitur

$$\Delta = \Sigma \pm \left(\frac{\partial x}{\partial w_m}\right)\left(\frac{\partial x_1}{\partial w_{m+1}}\right) \dots \left(\frac{\partial x_{n-m}}{\partial w_n}\right)\left(\frac{\partial x_{n-m+1}}{\partial \alpha}\right)\left(\frac{\partial x_{n-m+2}}{\partial \alpha_1}\right) \dots \left(\frac{\partial x_n}{\partial \alpha_{m-1}}\right)$$

$$= \left\{\Sigma \pm \frac{\partial w_m}{\partial x} \cdot \frac{\partial w_{m+1}}{\partial x_1} \dots \frac{\partial w_n}{\partial x_{n-m}} \cdot \frac{\partial w}{\partial x_{n-m+1}} \cdot \frac{\partial w_1}{\partial x_{n-m+2}} \dots \frac{\partial w_{m-1}}{\partial x_n}\right\}^{-1}$$

Quae est Propositio in theoria Multiplicatoris fundamentalis. Determinans inversum, quo Δ exprimitur, sic quoque scribi potest,

$$\left\{\Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \dots \frac{\partial w_n}{\partial x_n}\right\}^{-1}$$

cum permutatione functionum w, w_1 etc. valor Determinantis tantum signum mutare queat, quod hic non curamus.

Pro ipsis $w_m, w_{m+1}, \dots w_n$ etiam $n-m+1$ quantitates e numero ipsarum $x, x_1, \dots x_n$ sumere licet. Si statuimus

$$w_m = x, \quad w_{m+1} = x_1, \quad \dots \quad w_n = x_{n-m},$$

fit,

$$10. \quad \Delta = \Sigma \pm \left(\frac{\partial x_{n-m+1}}{\partial \alpha}\right)\left(\frac{\partial x_{n-m+2}}{\partial \alpha_1}\right) \dots \left(\frac{\partial x_n}{\partial \alpha_{m-1}}\right)$$

$$= \left\{\Sigma \pm \frac{\partial w}{\partial x_{n-m+1}} \cdot \frac{\partial w_1}{\partial x_{n-m+2}} \dots \frac{\partial w_{m-1}}{\partial x_n}\right\}^{-1}.$$

Porro e (4.) obtinetur,

$$W_m = X, \quad W_{m+1} = X_1, \quad \dots \quad W_n = X_{n-m}.$$

Hinc eruitur

Propositio II.

„Aequationum differentialium

$$dx : dx_1 \ldots . : dx_n = X : X_1 \ldots . : X_n,$$

quarum M est Multiplicator, inventis m Integralibus,

$$w = \alpha,\quad w_1 = \alpha_1,\quad \ldots . \quad w_{m-1} = \alpha_{m-1},$$

si exhibentur x_{n-m+1}, x_{n-m+2}, ... x_n per x, x_1, ... x_{n-m} atque Constantes Arbitrarias α, α_1, ... α_{m-1}, aequationum differentialium reductarum

$$dx : dx_1 \ldots . : dx_{n-m} = X : X_1 \ldots . : X_{n-m},$$

evadit Multiplicator,

$$M \Sigma \pm \left(\frac{\partial x_{n-m+1}}{\partial \alpha}\right)\left(\frac{\partial x_{n-m+2}}{\partial \alpha_1}\right) \ldots . \left(\frac{\partial x_n}{\partial \alpha_{m-1}}\right)$$

$$= M \left\{ \Sigma \pm \frac{\partial w}{\partial x_{n-m+1}} \cdot \frac{\partial w_1}{\partial x_{n-m+2}} \ldots . \frac{\partial w_{m-1}}{\partial x_n} \right\}^{-1}.\text{“}$$

Si eaedem aequationes differentiales propositae per diversa Integralium systemata reducuntur, Multiplicatores diversorum aequationum differentialium reductarum systematum ex eorum uno deduci possunt. Qua in re semper supponitur, unumquodque Integrale quod reductioni inservit sua affici Constante Arbitraria, ideoque aequationes differentiales reductas omnes ingredi Constantes Arbitrarias, quibus Integralia quorum ope reductio effecta est afficiuntur.

Sint enim rursus Integralia reductioni adhibenda,

$$w = \alpha,\quad w_1 = \alpha_1,\quad \ldots . \quad w_{m-1} = \alpha_{m-1},$$

atque aequationes differentiales reductae, inter variabiles w_m, w_{m+1}, ... w_n exhibitae,

$$11.\quad dw_m : dw_{m+1} \ldots . : dw_n = W_m : W_{m+1} \ldots . : W_n.$$

Eaedem aequationes differentiales propositae (1.) ope Integralium,

$$u = \beta,\quad u_1 = \beta_1,\quad \ldots . \quad u_{k-1} = \beta_{k-1},$$

reducantur ad has, inter variabiles u_k, u_{k+1}, ... u_n exhibitas,

$$12.\quad du_k : du_{k+1} \ldots . : du_n = U_k : U_{k+1} \ldots . : U_n.$$

Sit M Multiplicator aequationum differentialium propositarum, sint respective N et K Multiplicatores aequationum differentialium reductarum (11.) et (12.): erit secundum Prop. I.

$$13.\quad N = M \left\{ \Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \ldots . \frac{\partial w_n}{\partial x_n} \right\}^{-1},$$

$$K = M \left\{ \Sigma \pm \frac{\partial u}{\partial x} \cdot \frac{\partial u_1}{\partial x_1} \ldots . \frac{\partial u_n}{\partial x_n} \right\}^{-1},$$

unde

$$14. \quad K = N \frac{\Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots \frac{\partial w_n}{\partial x_n}}{\Sigma \pm \frac{\partial u}{\partial x} \cdot \frac{\partial u_1}{\partial x_1} \cdots \frac{\partial u_n}{\partial x_n}}.$$

Quae formula supponit, in aequationibus differentialibus reductis (11.) et (12.) ita definiri quantitates differentialibus proportionales ut fiat,

$$\frac{\partial w_m}{W_m} = \frac{\partial u_k}{U_k}.$$

Si ipsae $w, w_1, \ldots w_n$ per $u, u_1, \ldots u_n$ exprimuntur, formulam (14.) notae propositionis beneficio (D. F. §. 10. (5.)) concinnius sic exhibere licet,

$$15. \quad K = N\Sigma \pm \frac{\partial w}{\partial u} \cdot \frac{\partial w_1}{\partial u_1} \cdots \frac{\partial w_n}{\partial u_n}.$$

Quae formula generalis duos amplectitur casus, quo aequationes differentiales propositae per eadem Integralia reducuntur, sed reductae inter diversas variabiles exhibentur, et quo per diversa Integralia reductae inter easdem variabiles exhibentur.

Etenim ponendo $k = m$ atque

$$u = w, \quad u_1 = w_1, \quad \ldots \quad u_{m-1} = w_{m-1},$$

sequitur e (15.), si eaedem aequationes differentiales propositae per eadem Integralia,

$$w = \alpha, \quad w_1 = \alpha_1, \quad \ldots \quad w_{m-1} = \alpha_{m-1},$$

reducantur ad $n-m$ aequationes differentiales inter $n-m+1$ variabiles w_m, $w_{m+1}, \ldots w_n$ vel ad alias inter variabiles $u_m, u_{m+1}, \ldots u_n$, fieri

$$16. \quad K = N\Sigma \pm \frac{\partial w_m}{\partial u_m} \cdot \frac{\partial w_{m+1}}{\partial u_{m+1}} \cdots \frac{\partial w_n}{\partial u_n},$$

ubi $w_m, w_{m+1}, \ldots w_n$ expressae supponuntur per variabiles $u_m, u_{m+1}, \ldots u_n$ atque Constantes Arbitrarias $\alpha, \alpha_1, \ldots \alpha_{m-1}$.

Si vero rursus $k = m$ atque

$$u_m = w_m, \quad u_{m+1} = w_{m+1}, \quad \ldots \quad u_n = w_n,$$

vel si aequationes differentiales propositae per hoc m Integralium systema

$$w = \alpha, \quad w_1 = \alpha_1, \quad \ldots \quad w_{m-1} = \alpha_{m-1},$$

aut per hoc,

$$u = \beta, \quad u_1 = \beta_1, \quad \ldots \quad u_{m-1} = \beta_{m-1},$$

reducuntur ad $n-m$ aequationes differentiales diversas inter easdem $n-m+1$ variabiles $w_m, w_{m+1}, \ldots w_n$: abit formula (15.) in hanc,

$$17. \quad K = N\Sigma \pm \frac{\partial w}{\partial \beta} \cdot \frac{\partial w_1}{\partial \beta_1} \cdots \frac{\partial w_{m-1}}{\partial \beta_{m-1}},$$

siquidem in formando Determinante Functionali supponitur expressas esse w, w_1, ... w_{m-1} per variabiles w_m, w_{m+1}, ... w_n atque Constantes Arbitrarias β, β_1, ... β_m.

Principium ultimi Multiplicatoris sive quomodo cognito Multiplicatore systematis aequationum differentialium vulgarium ultima integratio ad Quadraturas revocatur.

§. 11.

Propositionum I. et. II. §. pr. prae ceteris memorabilis est casus $m = n-1$, quo omnibus praeter unum inventis Integralibus una integranda restat aequatio differentialis primi ordinis inter duas variabiles. Eo casu Multiplicator aequationis differentialis reductae redit in Multiplicatorem ***Eulerianum***, qui eam per se integrabilem reddit sive ad Quadraturas revocat. Unde ponendo $n = m-1$ e Propp. I. et II. §. pr. memorabiles prodeunt Propositiones, quae novum constituunt principium, e quo Calculus Integralis haud parum incrementi capit. Quod ***principium ultimi Multiplicatoris*** appellare convenit.

Propositio I.

„***Propositis aequationibus differentialibus***

$$dx : dx_1 \dots : dx_n = X : X_1 \dots : X_n$$

habeatur Multiplicator M sive solutio quaecunque aequationis differentialis partialis,

$$\frac{\partial . MX}{\partial x} + \frac{\partial . MX_1}{\partial x_1} \dots + \frac{\partial . MX_n}{\partial x_n} = 0;$$

porro inventa sint Integralia praeter unum omnia,

$$w = \alpha, \quad w_1 = \alpha_1, \quad \dots \quad w_{n-2} = \alpha_{n-2},$$

designantibus α etc. Constantes Arbitrarias, quibus ipsae functiones w, w₁ etc. non afficiantur; sumtis ex arbitrio duabus ipsarum x, x₁, ... xₙ functionibus wₙ₋₁, wₙ, fiat,

$$X\frac{\partial w_{n-1}}{\partial x} + X_1\frac{\partial w_{n-1}}{\partial x_1} \dots + X_n\frac{\partial w_{n-1}}{\partial x_n} = W_{n-1},$$

$$X\frac{\partial w_n}{\partial x} + X_1\frac{\partial w_n}{\partial x_1} \dots + X_n\frac{\partial w_n}{\partial x_n} = W_n,$$

erit ultimum Integrale

$$\int \frac{M\{W_n dw_{n-1} - W_{n-1} dw_n\}}{\Sigma \pm \frac{\partial w}{\partial x} . \frac{\partial w_1}{\partial x_1} \dots \frac{\partial w_n}{\partial x_n}} = \text{Const.}"$$

Propositio II.

„***Inventis aequationum differentialium,***

$$dx : dx_1 \dots : dx_n = X : X_1 \dots : X_n,$$

Integralibus praeter unum omnibus,

$$w = \alpha,\quad w_1 = \alpha_1,\quad \ldots\ldots\quad w_{n-2} = \alpha_{n-2},$$

ac designante M solutionem quamcunque aequationis differentialis partialis,

$$0 = \frac{\partial . MX}{\partial x} + \frac{\partial . MX_1}{\partial x_1} \ldots\ldots + \frac{\partial . MX_n}{\partial x_n},$$

exprimantur

$$x_2,\quad x_3,\quad \ldots\ldots\quad x_n,\quad X,\quad X_1,\quad M$$

per x et x_1 atque Constantes Arbitrarias

$$\alpha,\quad \alpha_1,\quad \ldots\ldots\quad \alpha_{n-2}:$$

erit ultima aequatio integralis,

$$\int \frac{M\{X_1 dx - X dx_1\}}{\Sigma \pm \frac{\partial w}{\partial x_2} . \frac{\partial w_1}{\partial x_3} \ldots\ldots \frac{\partial w_{n-2}}{\partial x_n}} = \text{Const."}$$

In duabus Propositionibus antecedentibus quantitas sub integrationis signo posita evadit differentiale completum, ubi expressiones in bina differentialia ducta per easdem duas variabiles exhibentur inter quas aequatio differentialis reducta locum habet. Similiter in sequentibus etsi pressis verbis non adnotetur, quoties formula integralis Constanti Arbitrariae aequiparatur, innuitur sub signo integrationis haberi differentiale completum.

In Propp. antecedentibus loco divisionis per Determinantia Functionalia,

$$\Sigma \pm \frac{\partial w}{\partial x} . \frac{\partial w_1}{\partial x_1} \ldots\ldots \frac{\partial w_n}{\partial x_n},$$

$$\Sigma \pm \frac{\partial w}{\partial x_2} . \frac{\partial w_1}{\partial x_3} \ldots\ldots \frac{\partial w_{n-2}}{\partial x_n},$$

etiam multiplicatio institui potuisset per Determinantia Functionalia sensu inverso formata (Det. Funct. §. 9.). Quod ubi fit, erit in altera Propositione ultima aequatio integralis,

$$1.\quad \int M\Delta (W_n\, dw_{n-1} - W_{n-1}\, dw_n) = \text{Const.},$$

posito

$$2.\quad \Delta = \Sigma \pm \frac{\partial x_2}{\partial \alpha} . \frac{\partial x_3}{\partial \alpha_1} \ldots\ldots \frac{\partial x_n}{\partial \alpha_{n-2}} . \frac{\partial x}{\partial w_{n-1}} . \frac{\partial x_1}{\partial w_n}$$

$$= \left\{ \Sigma \pm \frac{\partial w}{\partial x} . \frac{\partial w_1}{\partial x_1} \ldots\ldots \frac{\partial w_n}{\partial x_n} \right\}^{-1},$$

vel in altera

$$3.\quad \int M\Delta (X_1 dx - X dx_1) = \text{Const.},$$

posito

$$4.\quad \Delta = \Sigma \pm \frac{\partial x_2}{\partial \alpha} . \frac{\partial x_3}{\partial \alpha_1} \ldots\ldots \frac{\partial x_n}{\partial \alpha_{n-2}} = \left\{ \Sigma \pm \frac{\partial w}{\partial x_2} . \frac{\partial w_1}{\partial x_3} \ldots\ldots \frac{\partial w_{n-2}}{\partial x_n} \right\}^{-1}.$$

In formandis Determinantibus functionalibus (2.) et (4.) supponitur, aut ipsa $n-2$ Integralia dari novasque quoque variabiles w_{n-1}, w_n per x, x_1, ... x_n expressas esse, aut per integrationes transactas variabiles omnes expressas esse per binas w_{n-1}, w_n vel x, x_1 atque per Constantes Arbitrarias quae singulis integrationibus accedunt. Generalius si reductio ad aequationem differentialem primi ordinis inter duas variabiles efficitur ope $n-1$ aequationum integralium quarumcunque,

$$\Pi = 0, \quad \Pi_1 = 0, \quad \ldots. \quad \Pi_{n-2} = 0,$$

quae afficiuntur totidem Constantibus Arbitrariis

$$\alpha, \quad \alpha_1, \quad \ldots. \quad \alpha_{n-2},$$

poni poterit in formula (2.)

$$5. \quad \varDelta = \frac{\Sigma \pm \frac{\partial \Pi}{\partial \alpha} \cdot \frac{\partial \Pi_1}{\partial \alpha_1} \cdots\cdots \frac{\partial \Pi_{n-2}}{\partial \alpha_{n-2}}}{\Sigma \pm \frac{\partial \Pi}{\partial x_2} \cdot \frac{\partial \Pi_1}{\partial x_3} \cdots\cdots \frac{\partial \Pi_{n-2}}{\partial x_n} \cdot \frac{\partial w_{n-1}}{\partial x} \cdot \frac{\partial w_n}{\partial x_1}},$$

vel in formula (4.),

$$6. \quad \varDelta = \frac{\Sigma \pm \frac{\partial \Pi}{\partial \alpha} \cdot \frac{\partial \Pi_1}{\partial \alpha_1} \cdots\cdots \frac{\partial \Pi_{n-2}}{\partial \alpha_{n-2}}}{\Sigma \pm \frac{\partial \Pi}{\partial x_2} \cdot \frac{\partial \Pi_1}{\partial x_3} \cdots\cdots \frac{\partial \Pi_{n-2}}{\partial x_n}}$$

(Cf. *Det. Funct.* §. 10.). Formula antecedens prae ceteris cum fructu adhibetur. Aequationibus enim integralibus inventis saepissime per varias eliminationes eiusmodi formas induere licet, pro quibus Determinantia functionalia, quae numeratorem et denominatorem fractionis antecedentis constituunt, sine molestia inveniantur. Commode etiam adhiberi potest ad Determinantia functionalia formanda propositio, valorem Determinantium functionalium,

$$\Sigma \pm \frac{\partial w}{\partial x} \cdot \frac{\partial w_1}{\partial x_1} \cdots\cdots \frac{\partial w_n}{\partial x_n}, \qquad \Sigma \pm \frac{\partial w}{\partial x_2} \cdot \frac{\partial w_1}{\partial x_3} \cdots\cdots \frac{\partial w_{n-2}}{\partial x_n},$$

non mutari, si ante differentiationes partiales transigendas functio quaeque w_i ope aequationum,

$$7. \quad w = \alpha, \quad w_1 = \alpha_1, \quad \ldots. \quad w_{i-1} = \alpha_{i-1},$$

mutationes quascunque subeat. Inservire possunt aequationes (7.) ad eliminandas e quaque functione w_i variabiles

$$x_n, \quad x_{n-1}, \quad \ldots. \quad x_{n-i+1}.$$

Quo facto si abit w_i in Π_i, erunt

$$\Pi - \alpha = 0, \quad \Pi_1 - \alpha_1 = 0, \quad \ldots. \quad \Pi_{n-2} - \alpha_{n-2} = 0,$$

aequationes integrales, quales per integrationem et eliminationem successivam

inveniuntur. Porro fit

$$8.\quad X \pm \frac{\partial w}{\partial x_2}\cdot\frac{\partial w_1}{\partial x_3}\cdots\frac{\partial w_{n-2}}{\partial x_n} = \frac{\partial \Pi}{\partial x_n}\cdot\frac{\partial \Pi_1}{\partial x_{n-1}}\cdots\frac{\partial \Pi_{n-2}}{\partial x_2}.$$

Cf. §. 3. Si vero adhibentur variabilium expressiones quales ex eliminatione successiva prodeunt, videlicet ipsius x_n expressio per $x, x_1, \ldots x_{n-1}, \alpha$; ipsius x_{n-1} expressio per $x, x_1, \ldots x_{n-2}, \alpha, \alpha_1$ etc., abit Determinans

$$X \pm \frac{\partial x_2}{\partial \alpha}\cdot\frac{\partial x_3}{\partial \alpha_1}\cdots\frac{\partial x_n}{\partial \alpha_{n-2}}$$

in productum

$$\left(\frac{\partial x_n}{\partial \alpha}\right)\left(\frac{\partial x_{n-1}}{\partial \alpha_1}\right)\cdots\left(\frac{\partial x_2}{\partial \alpha_{n-2}}\right),$$

ubi uncis innuo esse x_{n-i} ipsarum $x, x_1, \ldots x_{n-i-1}, \alpha, \alpha_1, \ldots \alpha_i$ functionem. Quibus substitutis in (4.), fit

$$9.\quad \Delta = \left(\frac{\partial x_n}{\partial \alpha}\right)\left(\frac{\partial x_{n-1}}{\partial \alpha_1}\right)\cdots\left(\frac{\partial x_2}{\partial \alpha_{n-2}}\right) = \frac{1}{\frac{\partial \Pi}{\partial x_n}\cdot\frac{\partial \Pi_1}{\partial x_{n-1}}\cdots\frac{\partial \Pi_{n-2}}{\partial x_2}}.$$

Hinc sequentes emergunt Propositiones.

Propositio III.

„Aequationum differentialium vulgarium,

$$dx : dx_1 \ldots : dx_n = X : X_1 \ldots : X_n,$$

quarum M est Multiplicator, inventis per integrationem et eliminationem successivam aequationibus integralibus praeter unam omnibus,

$$\Pi = \alpha,\quad \Pi_1 = \alpha_1,\quad \ldots\quad \Pi_{n-2} = \alpha_{n-2},$$

ubi Π_i est functio variabilium $x, x_1, \ldots x_{n-i}$ atque Constantium Arbitrariarum $\alpha, \alpha_1, \ldots \alpha_{i-1}$: fit ultima aequatio integralis,

$$\int \frac{M\{X_1\,dx - X\,dx_1\}}{\frac{\partial \Pi}{\partial x_n}\cdot\frac{\partial \Pi_1}{\partial x_{n-1}}\cdots\frac{\partial \Pi_{n-2}}{\partial x_2}} = \text{Const.“}$$

Propositio IV.

„Aequationum differentialium vulgarium

$$dx : dx_1 \ldots : dx_n = X : X_1 \ldots : X_n,$$

quarum M est Multiplicator, inventis per integrationem et eliminationem successivam expressionibus ipsius x_n per $x, x_1, \ldots x_{n-1}$ atque Constantem Arbitrariam α; ipsius x_{n-1} per $x, x_1, \ldots x_{n-2}$ atque Constantes Arbitrarias α, α_1 etc., denique ipsius x_2 per x, x_1 atque Constantes Arbitrarias $\alpha, \alpha_1, \ldots \alpha_{n-2}$, dabitur aequatio inter x et x_1 per formulam,

$$\int \left(\frac{\partial x_n}{\partial \alpha}\right)\left(\frac{\partial x_{n-1}}{\partial \alpha_1}\right)\cdots\left(\frac{\partial x_2}{\partial \alpha_{n-2}}\right) M(X_1\,dx - X\,dx_1) = \text{Const.“}$$

In utraque Propositione functiones sub signo integrationis ope aequationum integralium inventarum per x et x_1 exprimendae sunt.

Quod e Multiplicatore aequationum differentialium propositarum eruitur Multiplicator aequationis differentialis, in quam post inventa praeter unum omnia Integralia problema redit, id eo maioris momenti est, quia huius ultimae aequationis differentialis primi ordinis inter duas variabiles valde latere potest Multiplicator, dum systematis aequationum differentialium propositarum sponte se offert. Veluti quod in gravissimis quaestionibus evenit, si ipsarum X, X_1 etc. expressiones ita sunt comparatae, ut identice habeatur,

$$\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \dots + \frac{\partial X_n}{\partial x_n} = 0,$$

aequationum differentialium propositarum Multiplicator *unitati* aequalis evadit; aequationis autem postremo integrandae Multiplicator secundum antecedentia aequatur Determinanti Functionali, cui valor complicatus competere potest. Casu illo particulari in quatuor Propositionibus antecedentibus ponere licet $M = 1$; quod ubi ex gr. in Prop. IV. facimus, emergit haec:

Propositio V.

„*Proponantur aequationes differentiales simultaneae,*

$$dx : dx \dots : dx_n = X : X_1 \dots : X_n,$$

designantibus X, X_1, etc. variabilium x, x_1 etc. functiones pro quibus identice habeatur,

$$\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \dots + \frac{\partial X_n}{\partial x_n} = 0;$$

inventis aequationum propositarum $n-1$ Integralibus, $n-1$ Constantes Arbitrarias α, α_1, ... α_{n-2} involventibus, exprimantur X et X_1 atque variabiles x_2, x_3, ... x_n per x, x_1 atque istas Constantes Arbitrarias α, α_1, ... α_{n-2}: erit ultimum Integrale,

$$\int \left(\Sigma \pm \frac{\partial x_2}{\partial \alpha} \cdot \frac{\partial x_3}{\partial \alpha_1} \dots \frac{\partial x_n}{\partial \alpha_{n-2}} \right) \left\{ X_1 dx - X dx_1 \right\} = \text{Const.},$$

ubi expressio sub integrationis signo differentiale completum existit."

Propositionis antecedentis afferam exempla pro $n = 2$ et $n = 3$.

I. „Proponantur aequationes differentiales

$$dx : dy : dz = X : Y : Z,$$

designantibus X, Y, Z variabilium x, y, z functiones, pro quibus identice fiat,

$$\frac{\partial X}{\partial x} + \frac{\partial Y}{\partial y} + \frac{\partial Z}{\partial z} = 0;$$

invento uno Integrali involvente Constantem Arbitrariam α, exprimantur X, Y, z per x, y, α, erit alterum Integrale,

$$\int \frac{\partial z}{\partial \alpha} \{Ydx - Xdy\} = \text{Const."}$$

II. „Proponantur aequationes differentiales

$$dt:dx:dy:dz = T:X:Y:Z,$$

designantibus T, X, Y, Z variabilium t, x, y, z functiones, pro quibus identice fiat,

$$\frac{\partial T}{\partial t} + \frac{\partial X}{\partial x} + \frac{\partial Y}{\partial y} + \frac{\partial Z}{\partial z} = 0,$$

inventis duobus Integralibus involventibus Constantes Arbitrarias α et β, exprimantur T, X, y, z per t, x, α, β; erit tertium Integrale,

$$\int \left(\frac{\partial y}{\partial \alpha} \cdot \frac{\partial z}{\partial \beta} - \frac{\partial y}{\partial \beta} \cdot \frac{\partial z}{\partial \alpha}\right) (Xdt - Tdx) = \text{Const."}$$

Quae exempla non sine molesto calculo verificantur.

Quibus casibus Multiplicator aequationum differentialium per aequationes integrales *particulares* reductarum ex aequationum differentialium propositarum Multiplicatore eruitur. Principium ultimi Multiplicatoris siue Determinantium adiumento comprobatum.

§. 12.

Si aequationes integrales, aequationibus differentialibus reducendis adhibitae, sunt particulares, in genere non licet Multiplicatorem aequationum differentialium reductarum e Multiplicatore propositarum deducere. In Prop. II. §. 10., quae docet quomodo aequationum differentialium propositarum et reductarum Multiplicatores a se invicem pendeant, possunt quidem Constantibus Arbitrariis quibus Integralia afficiuntur valores particulares tribui: supponitur autem ipsa cognita esse aequationum differentialium propositarum Integralia generalia. Quae tamen suppositio necessaria non est. Etenim si aequationes integrales reductioni adhibendae alia post aliam investigantur, sufficit unamquamque aequationem integralem inventam ita comparatam esse, ut differentiata per aequationes differentiales propositas identica reddatur, simul omnibus *ipsam praecedentibus* aequationibus integralibus accitis. Neque vero propositum succederet si ex aequationibus integralibus reductioni adhibitis duae pluresve ita comparatae essent, ut quaeque earum differentiata per aequationes differentiales propositas identica reddi non possit nisi simul omnes reliquae aequationes integrales, nullo ordine observato, in auxilium vocentur.

Antecedentia cum e formulis traditis patent tum ope propositionis elementaris directe demonstrantur, quoties aequationes integrales alia post aliam inventae ad variabiles successive eliminandas adhibentur. Sit enim aequationum differentialium propositarum primum Integrale inventum,

$$F = \alpha;$$

cujus ope e quantitatibus X, X_1, ... X_{n-1} eliminetur x_n. Ponendo $m=1$ in Prop. II §. 10. sequitur, *Multiplicatorem aequationum differentialium reductarum,*

$$1. \quad dx : dx_1 \dots : dx_{n-1} = X : X_1 \dots : X_{n-1},$$

aequari Multiplicatori aequationum differentialium propositarum diviso per $\frac{\partial F}{\partial x_n}$ *sive quantitati*

$$\frac{M}{\frac{\partial F}{\partial x_n}},$$

in qua variabilis x_n per aequationem $F=\alpha$ eliminanda est. Constans α in hac propositione fundamentali arbitraria est ideoque valor ei quicunque tribui potest particularis.

Tributo in functionibus X, X_1, ... X_{n-1} Constanti α quam implicant valore particulari, sit aequationum (1.) Integrale,

$$F_1 = \alpha_1.$$

Quod non erit Integrale aequationum differentialium propositarum. Quippe aequatio $dF_1=0$ per aequationes differentiales propositas identica non redditur nisi simul Constans α ubique functioni F aequatur. Quae Constantis α eliminatio ubi fit in functione F_1, aequatio $F_1=\alpha_1$ evadit Integrale aequationum differentialium propositarum. Sed ea Constantis α eliminatio fieri non potest si ei in aequationibus differentialibus reductis (1.) tribuitur valor particularis, neque igitur eo casu ex aequationum differentialium reductarum Integrali Integrale propositarum restituere licet.

Eliminata x_{n-1} ope aequationis $F_1=\alpha_1$, obtinentur e (1.) aequationes differentiales denuo reductae,

$$2. \quad dx : dx_1 \dots dx_{n-2} = X : X_1 \dots : X_{n-2}.$$

Quarum Multiplicator secundum eandem regulam derivatur e Multiplicatore aequationum (1.), atque hic e Multiplicatore aequationum differentialium propositarum erutus est, videlicet dividendo per $\frac{\partial F_1}{\partial x_{n-1}}$, unde prodit aequationum (2.) Multiplicator,

$$\frac{M}{\frac{\partial F_1}{\partial x_n}\cdot\frac{\partial F_1}{\partial x_{n-1}}},$$

quae quantitas variabilibus x_n et x_{n-1} per aequationes $F=\alpha$, $F_1=\alpha_1$ eliminatis solarum $x, x_1, \ldots. x_{n-2}$ functio evadit. Unde aequationum differentialium (2.) erutus est Multiplicator, quamquam reductio facta est per duas aequationes $F=\alpha$, $F_1=\alpha_1$, quarum tantum altera est aequationum differentialium propositarum Integrale, altera non est neque ad tale revocari potest, si Constanti α tributus est valor particularis.

Rursus tributo Constanti α_1 valore particulari quocunque, aequationum (2.) quaeratur Integrale, quo invento aequationes differentiales (2.) ulterius reduci possunt, reductarumque per eandem regulam constabit Multiplicator. Sic pergendo successive eruantur m aequationes integrales,

$$3.\qquad F=\alpha,\quad F_1=\alpha_1,\quad \ldots.\quad F_{m-1}=\alpha_{m-1},$$

in quibus $\alpha, \alpha_1, \ldots. \alpha_{m-1}$ sint Constantes particulares quaecunque; quarum aequationum integralium ope revocatis $X, X_1, \ldots. X_{n-m}$ ad solarum x, $x_1, \ldots. x_{n-m}$ functiones, aequationum differentialium ad quas successiva eliminatione pervenitur,

$$4.\qquad dx:dx_1\ldots.:dx_{n-m}=X:X_1\ldots.:X_{n-m},$$

eruitur Multiplicator,

$$5.\qquad \frac{M}{\frac{\partial F}{\partial x_n}\cdot\frac{\partial F_1}{\partial x_{n-1}}\cdots\frac{\partial F_{m-1}}{\partial x_{n-m+1}}},$$

quae quantitas et ipsa per aequationes (3.) ad solarum $x, x_1, \ldots. x_{n-m}$ functionem revocanda est. Aequationes (3.) reductionibus successivis inservientes hic ita comparatae sunt ut quaeque $F_i=\alpha_i$ sit Integrale aequationum differentialium,

$$dx:dx_1\ldots\;:dx_{n-i}=X:X_1\ldots.:X_{n-i},$$

variabilibus $x_n, x_{n-1}, \ldots. x_{n-i+1}$ e $X, X_1, \ldots. X_{n-i}$ eliminatis ope aequationum ipsam $F_i=\alpha_i$ praecedentium,

$$F=\alpha,\quad F_1=\alpha_1,\quad \ldots.\quad F_{i-1}=\alpha_{i-1}.$$

Si $m=n-1$, formula (5.) suppeditat Multiplicatorem aequationis differentialis primi ordinis inter duas variabiles x et x_1,

$$6.\qquad X_1dx-Xdx_1=0,$$

quae post inventas aequationes integrales,

$$7.\qquad F=\alpha,\quad F_1=\alpha_1,\quad \ldots.\quad F_{n-2}=\alpha_{n-2},$$

unica integranda restat. Multiplicatore sic invento,

$$\frac{M}{\frac{\partial F}{\partial x_n}\cdot\frac{\partial F_1}{\partial x_{n-1}}\cdots\frac{\partial F_{n-2}}{\partial x_2}},$$

laeva pars aequationis (6.) evadit differentiale completum, unde eius integratio ad Quadraturas revocatur sive fit ultima aequatio integralis,

$$8.\quad \int\frac{M(X_1\,dx-X\,dx_1)}{\frac{\partial F}{\partial x_n}\cdot\frac{\partial F_1}{\partial x_{n-1}}\cdots\frac{\partial F_{n-2}}{\partial x_2}} = \text{Const.}$$

Qua in formula adiumento aequationum integralium inventarum (7.) quantitates sub integrationis signo in differentialia dx et dx_1 ductae, per solas x et x_1 exprimendae sunt.

Cum antecedentibus Constantes α, α_1, ... α_{n-2} sint particulares *quaecunque*, earum valorem etiam generalem seu indefinitam servare licet, quo facto formula (8.) redit in Prop. III. §. pr. Vice versa Prop. III. §. pr., in qua designant α, α_1, ... α_{n-2} Constantes Arbitrarias, eum quoque amplectitur casum quo post quamque novam integrationem Constanti Arbitrariae qua afficitur valor tribuitur particularis. Quod intelligitur observando, aequationibus differentialibus Constantes Arbitrarias involventibus, idem earum Integrale obtineri posse, sive ante sive post integrationem Constantibus Arbitrariis illis valores particulares tribuas.

Necessarium non est, ut quaeque nova aequatio integralis inveniatur ut Integrale ipsarum aequationum differentialium ad quas propositae reducuntur eliminato per aequationes integrales ante inventas aequali variabilium numero; generalius ea esse poterit Integrale aequationum differentialium propositarum, per aequationes integrales ante ipsam inventas quocunque modo transformatarum. Aequationum enim differentialium propositarum per Integrale $F=\alpha$ transformatarum sit Integrale $F_1=\alpha_1$; aequationum differentialium propositarum per binas aequationes $F=\alpha$, $F_1=\alpha_1$ transformatarum sit Integrale $F_2=\alpha_2$, per tres aequationes $F=\alpha$, $F_1=\alpha_1$, $F_2=\alpha_2$ transformatarum sit Integrale $F_3=\alpha_3$, et ita porro, ubi Constantes α, α_1 etc. poterunt arbitrariae esse sive particulares quaecunque. Quibus positis, ex aequatione integrali $F=\alpha$ et aequationibus differentialibus propositis sequi debet, $dF_1=0$; unde per aequationem $F=\alpha$ eliminata x_n e functionibus X, X_1, ... X_{n-1}, F_1, fieri debet $F'_1=\alpha_1$ Integrale aequationum differentialium,

$$dx : dx_1 \;....: dx_{n-1} = X : X_1 \;.....\, X_{n-1}.$$

Ex aequationibus integralibus $F = \alpha$, $F_1 = \alpha_1$ et aequationibus differentialibus propositis sequi debet $dF_2 = 0$; unde per aequationes $F = \alpha$, $F_1 = \alpha_1$ eliminatis x_n et x_{n-1} e functionibus X, X_1, ... X_{n-2}, fieri debet $F_2 = \alpha_2$ Integrale aequationum differentialium,

$$dx : dx_1 \ldots : dx_{n-2} = X : X_1 \ldots : X_{n-2},$$

et ita porro. Generaliter si primum functiones F_1, F_2 etc. ratione illa generaliori qua eas definivi obtinebantur, ac deinde e quaque F_i eliminantur x_n, x_{n-1}, ... x_{n-i+1} per aequationes $F = \alpha$, $F_1 = \alpha_1$, ... $F_{i-1} = \alpha_{i-1}$, eaedem functiones F, F_1, F_2 etc. prodeunt quas in formulis (5. et. 8.) consideravi. Ea autem reductione adhibita abit Determinans functionale

$$\Sigma \pm \frac{\partial F}{\partial x_n} \cdot \frac{\partial F_1}{\partial x_{n-1}} \cdots \frac{\partial F_{m-1}}{\partial x_{n-m+1}}$$

in simplex productum

$$\frac{\partial F}{\partial x_n} \cdot \frac{\partial F_1}{\partial x_{n-1}} \cdots \frac{\partial F_{m-1}}{\partial x_{n-m+1}},$$

quod formulae (5.) denominatorem afficit (§. 3.). Unde si functionibus F, F_1, F_2 etc. generaliorem significatum servare placet, formula (5.) evadere debet,

$$9. \qquad \frac{M}{\Sigma \pm \frac{\partial F}{\partial x_n} \cdot \frac{\partial F_1}{\partial x_{n-1}} \cdots \frac{\partial F_{m-1}}{\partial x_{n-m+1}}},$$

ideoque etiam formula (8.)

$$10. \qquad \int \frac{M\{X_1 dx - X dx_1\}}{\Sigma \pm \frac{\partial F}{\partial x_n} \cdot \frac{\partial F_1}{\partial x_{n-1}} \cdots \frac{\partial F_{n-2}}{\partial x_2}} = \text{Const.}$$

Definitio functionum F, F_1 etc. amplectitur casum quo omnes aequationes $F_i = \alpha_i$ sunt ipsarum aequationum differentialium Integralia generalia. Unde e simplice propositione elementari tradita derivatur principium ultimi Multiplicatoris, si reductio ad aequationem differentialem primi ordinis inter duas variabiles per Integralia generalia fit, simulque monstrantur casus maxime generales quibus invenire liceat ultimum Multiplicatorem, etsi aequationes integrales reductioni adhibitae sint particulares.

Addam demonstrationem propositionis fundamentalis qua antecedentibus vidimus principium ultimi Multiplicatoris via maxime elementari adeoque absque ullo Determinantium adiumento superstrui.

Propositio.

„*Sit F solutio quaecunque aequationis*

$$X\frac{\partial F}{\partial x} + X_1\frac{\partial F}{\partial x_1} \cdots + X_n\frac{\partial F}{\partial x_n} = 0,$$

exclusa Constante; sit porro M solutio quaecunque aequationis

$$\frac{\partial.MX}{\partial x}+\frac{\partial.MX_1}{\partial x_1}\dots+\frac{\partial.MX_n}{\partial x_n}=0,$$

Constante non exclusa: posito

$$N=\frac{M}{\frac{\partial F}{\partial x_n}},$$

ipsisque N, X, X_1, ... X_{n-1} per x, x_1, ... x_{n-1}, F expressis, fit N solutio aequationis

$$\frac{\partial.NX}{\partial x}+\frac{\partial.NX_1}{\partial x_1}\dots+\frac{\partial.NX_{n-1}}{\partial x_{n-1}}=0."$$

Demonstratio.

Ponatur

$$\frac{\partial F}{\partial x_n}=u;$$

differentiando variabilis x_n respectu aequationem identicam,

$$X\frac{\partial F}{\partial x}+X_1\frac{\partial F}{\partial x_1}\dots+X_n\frac{\partial F}{\partial x_n}=0,$$

prodit,

$$X\frac{\partial u}{\partial x}+X_1\frac{\partial u}{\partial x_1}\dots+X_n\frac{\partial u}{\partial x_n}$$
$$+\frac{\partial X}{\partial x_n}\cdot\frac{\partial F}{\partial x}+\frac{\partial X_1}{\partial x_n}\cdot\frac{\partial F}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}\cdot\frac{\partial F}{\partial x_n}=0$$

Innuendo uncis quibus differentialia partialia includantur exhiberi X, X_1 etc. per x, x_1, ... x_{n-1}, F, fit

$$\frac{\partial X_i}{\partial x_n}=\left(\frac{\partial X_i}{\partial F}\right)\frac{\partial F}{\partial x_n}=\left(\frac{\partial X_i}{\partial F}\right)u.$$

Quam formulam in aequatione praecedente substituendo atque per u dividendo prodit,

$$X\frac{\partial\log u}{\partial x}+X_1\frac{\partial\log u}{\partial x_1}\dots+X_n\frac{\partial\log u}{\partial x_n}$$
$$+\left(\frac{\partial X}{\partial F}\right)\frac{\partial F}{\partial x}+\left(\frac{\partial X_1}{\partial F}\right)\frac{\partial F}{\partial x_1}\dots+\left(\frac{\partial X_n}{\partial F}\right)\frac{\partial F}{\partial x_n}=0.$$

Haec formula detrahatur de sequente, quae ex ea qua M definitur fluit,

$$X\frac{\partial\log M}{\partial x}+X_1\frac{\partial\log M}{\partial x_1}\dots+X_n\frac{\partial\log M}{\partial x_n}$$
$$+\frac{\partial X}{\partial x}+\frac{\partial X_1}{\partial x_1}\dots+\frac{\partial X_n}{\partial x_n}=0,$$

simulque observetur haberi pro indicis i valoribus 1, 2, ... $n-1$,

$$\frac{\partial X_i}{\partial x_i} = \left(\frac{\partial X_i}{\partial x_i}\right) + \left(\frac{\partial X_i}{\partial F}\right)\frac{\partial F}{\partial x_i},$$

prodit ponendo $\frac{M}{u} = N$,

$$X\frac{\partial \log N}{\partial x} + X_1\frac{\partial \log N}{\partial x_1}\dots + X_n\frac{\partial \log N}{\partial x_n}$$
$$+\left(\frac{\partial X}{\partial x}\right) + \left(\frac{\partial X_1}{\partial x_1}\right)\dots + \left(\frac{\partial X_{n-1}}{\partial x_{n-1}}\right) = 0$$

Fit autem

$$X\frac{\partial \log N}{\partial x} + X_1\frac{\partial \log N}{\partial x_1}\dots + X_n\frac{\partial \log N}{\partial x_n}$$
$$= X\left(\frac{\partial \log N}{\partial x}\right) + X_1\left(\frac{\partial \log N}{\partial x_1}\right)\dots + X_{n-1}\left(\frac{\partial \log N}{\partial x_{n-1}}\right)$$
$$+\frac{\partial \log N}{\partial F}\left\{X\frac{\partial F}{\partial x} + X_1\frac{\partial F}{\partial x_1}\dots + X_n\frac{\partial F}{\partial x_n}\right\}$$
$$= X\left(\frac{\partial \log N}{\partial x}\right) + X_1\left(\frac{\partial \log N}{\partial x_1}\right)\dots + X_{n-1}\left(\frac{\partial \log N}{\partial x_{n-1}}\right),$$

aggregato in $\left(\frac{\partial \log N}{\partial F}\right)$ ducto identice evanescente Unde aequatio antecedens sic quoque exhiberi potest:

$$X\left(\frac{\partial \log N}{\partial x}\right) + X_1\left(\frac{\partial \log N}{\partial x_1}\right)\dots + X_{n-1}\left(\frac{\partial \log N}{\partial x_{n-1}}\right)$$
$$+\left(\frac{\partial X}{\partial x}\right) + \left(\frac{\partial X_1}{\partial x_1}\right)\dots + \frac{\partial X_{n-1}}{\partial x_{n-1}} = 0.$$

quae per N multiplicata suppeditat,

$$\left(\frac{\partial . NX}{\partial x}\right) + \left(\frac{\partial . NX_1}{\partial x_1}\right)\dots + \left(\frac{\partial . NX_{n-1}}{\partial x_{n-1}}\right) = 0,$$

quae est formula demonstranda.

Vidimus supra, propositione antecedente iteratis vicibus adhibita erui aequationum differentialium reductarum Multiplicatorem e Multiplicatore propositarum. Sed ad hunc finem non necesse est ut hic ipse cognoscatur sed sufficit eius cognoscere valorem quem per aequationes integrales reductioni adhibitas induere potest. Si problema ad aequationem differentialem primi ordinis inter x et x_1 revocatum est, definitur M aequationibus,

$$11.\quad \frac{d\log M}{dx} = -\frac{1}{X}\left\{\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1}\dots + \frac{\partial X_n}{\partial x_n}\right\} X_1 dx = X dx_1,$$

in quibus *post differentiationes partiales factas* eliminandae sunt $x_2, x_3, \dots$ $\dots x_n$. Si aequationes integrales, quarum ope reductiones et eliminationes propositae operantur, particulares sunt, evenire potest ut e formulis (11.) eruatur valor ipsius M in principio ultimi Multiplicatoris requisitus, neque tamen

inveniri queat ipsius M valor generalis sive ipsarum aequationum differentialium propositarum Multiplicator. Directe aequationis differentialis,

$$X_1 dx - X dx_1 = 0,$$

definitur Multiplicator P per formulam,

$$12 \qquad \frac{d \log P}{dx} = -\frac{1}{X}\left\{\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1}\right\},$$

in cuius dextra parte X et X_1 *ante differentiationes partiales transigendas* per solas x et x_1 exprimendae sunt. Potest autem evenire ut via non pateat qua ipsum P e (12.) eruatur, dum ipsius M determinatio per formulam (11.) in promtu est. Quae adeo, nullis cognitis aequationibus integralibus, in amplis gravissimisque problematis succedit, unde pro quibuscunque aequationibus integralibus reductioni adhibitis sive completis sive dicta ratione inventis particularibus ultimus Multiplicator constat.

De usu Multiplicatoris in integrandis systematis quibusdam aequationum differentialium specialibus.

§. 13.

Systema aequationum differentialium propositarum ita comparatum esse potest ut ultima Integratio sponte in Quadraturam redeat. Quod evenit si unius variabili differentiale tantum, non ipsa in aequationibus differentialibus invenitur. Ponamus ipsam x esse variabilem a qua simul omnes functiones vacuae sint X, X_1, ... X_n: redire constat integrationem n aequationum differentialium inter $n+1$ variabiles,

$$1. \qquad dx : dx_1 : dx_2 \ldots : dx_n = X : X_1 : X_2 \ldots : X_n,$$

in integrationem $n-1$ aequationum differentialium inter n variabiles unamque Quadraturam. Integratis enim aequationibus,

$$2. \qquad dx_1 : dx_2 \ldots : dx_n = X_1 : X_2 \ldots : X_n,$$

quae sunt $n-1$ aequationes differentiales inter n variabiles x_1, x_2, ... x_n, exhiberi poterunt variabiles x_1, x_2, ... x_n per earum unam veluti x_1: unde, expressa $\frac{X}{X_1}$ per x_1, dabit simplex Quadratura ipsius x valorem,

$$3. \qquad x = \int \frac{X dx_1}{X_1} + \text{Const.}$$

Iam cognito aequationum differentialium (1.) Multiplicatore quaeritur, quemnam ex eo fructum ad integrationem perficiendam percipere liceat, cum ultima integratio sua sponte in Quadraturam redeat. Quod ut cognoscatur, inter duo casus distinguendum erit, prout datus aequationum differentialium (1.) Multiplicator a variabili x afficiatur sive non afficiatur.

Aequationum differentialium (2.) systema vocabo *proprium*, quo distinguatur a systemate *proposito* aequationum differentialium (1.), cuius integratio componitur ex integratione systematis proprii et Quadratura. Si datus systematis propositi Multiplicator M et ipse a variabili x vacuus est, idem erit systematis proprii Multiplicator. Tum enim evanescente termino $\frac{\partial . MX}{\partial x}$, satisfaciet aequationum differentialium (1.) Multiplicator aequationi,

$$\frac{\partial . MX_1}{\partial x_1} + \frac{\partial . MX_2}{\partial x_2} \ldots + \frac{\partial . MX_n}{\partial x_n} = 0,$$

eadem autem aequatione definitur aequationum differentialium (2.) Multiplicator. Quoties igitur datus systematis propositi (1.) Multiplicator et ipse variabili x vacat, systematis proprii ultima integratio ad Quadraturas revocari potest, sive quod idem est, ***systematis aequationum differentialium propositarum duae ultimae integrationes per Quadraturas absolvuntur.***

Vice versa si datur systematis proprii (2.) Multiplicator N, qui erit solarum variabilium $x_1, x_2, \ldots x_n$ functio, idem erit systematis propositi (1.) Multiplicator. Evanescente enim termino $\frac{\partial . NX}{\partial x}$, functio N, quae huic aequationi satisfacere debet,

$$0 = \frac{\partial . NX_1}{\partial x_1} + \frac{\partial . NX_2}{\partial x_2} \ldots + \frac{\partial . NX_n}{\partial x_n},$$

etiam huic satisfaciet qua systematis propositi Multiplicator definitur,

$$0 = \frac{\partial . NX}{\partial x} + \frac{\partial . NX_1}{\partial x_1} \ldots + \frac{\partial . NX_n}{\partial x_n}$$

Inventis autem omnibus systematis proprii Integralibus,

$$4. \quad f_1 = \alpha_1, \quad f_2 = \alpha_2, \quad \ldots \quad f_{n-1} = \alpha_{n-1},$$

ubi Constantes Arbitrariae α_1 etc. dextram aequationum partem occupant, erit aequationum (2.) Multiplicator,

$$5. \quad N = \frac{1}{X_n} \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \ldots \frac{\partial f_{n-1}}{\partial x_{n-1}}.$$

Qui igitur systematis quoque propositi Multiplicator erit. Unde si systematis propositi datur Multiplicator M, variabilem x implicans, simulque systema proprium complete integratum est, duo innotescunt systematis propositi Multiplicatores M et N. Quibus cognitis, secundum §. 4. systematis propositi constabit Integrale,

$$6. \quad \frac{N}{M} = \frac{1}{MX_n} \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \ldots \frac{\partial f_{n-1}}{\partial x_{n-1}} = \text{Const.}$$

Quo Integrali dabitur x per $x_1, x_2, \ldots. x_n$, sive ope Integralium (4.) expressis $x_2, x_3, \ldots. x_n$ per x_1, dabitur x per x_1. Unde *si innotescit systematis propositi Multiplicator variabili x affectus, post systematis proprii integrationem completam, non amplius opus erit Quadratura, quam formula* (3.) *poscebat ad inveniendum ipsius x valorem per x_1 expressum.*

Fieri potest ut solo cognito systematis propositi Multiplicatore variabili x affecto, absque ulla integratione eruantur systematis proprii unum plurave Integralia. Expressa enim per (4.) quantitate $\frac{X}{X_1}$ per $x_1, \alpha_1, \alpha_2, \ldots. \alpha_{n-1}$, in functione

$$\int \frac{X \partial x_1}{X_1},$$

post factam integrationem, Constantium α_1, α_2 etc. loco restituamus functiones f_1, f_2 etc., quo facto prodeat variabilium $x_1, x_2, \ldots. x_n$ functio

$$\xi = \int \frac{X\, dx_1}{X_1}:$$

erit e (3.), designante α_n novam Constantem Arbitrariam,

$$x - \xi = \alpha_n$$

systematis propositi Integrale. Sit rursus variabilium $x_1, x_2, \ldots. x_n$ functio N systematis proprii ideoque etiam systematis propositi Multiplicator, erit secundum §. 4. expressio generalis Multiplicatoris systematis propositi,

$$M = \Pi(x - \xi, f_1, f_2, \ldots. f_{n-1}).N.$$

Cognito igitur valor ipsius M, variabili x affecto, erit $\frac{\partial \log M}{\partial x}$ ipsarum $x - \xi$, $f_1, f_2, \ldots. f_{n-1}$ functio,

$$\frac{\partial \log M}{\partial x} = \Phi(x - \xi, f_1, f_2, \ldots. f_{n-1}).$$

Unde ponendo

$$7. \quad \frac{\partial \log M}{\partial x} = u,$$

atque ex hac aequatione quaerendo ipsius x valorem per $u, x_1, x_2, \ldots. x$ expressum, prodit

$$x = \xi + \psi(u, f_1, f_2, \ldots. f_{n-1}),$$

designante ψ certam ipsarum $u, f_1, f_2, \ldots. f_{n-1}$ functionem. Quaerendo igitur e (7.) ipsius x valorem per $u, x_1, x_2, \ldots. x_n$ expressum, atque in ea expressione ipsius u loco ponendo varios valores constantes arbitrarios, differentiae quantitatum provenientium erunt solarum $f_1, f_2, \ldots. f_n$ functiones, ideoque Constantibus Arbitrariis aequiparatae suppeditabunt systematis proprii

Integralia. Methodus hic tradita semper succedit si non tantum M sed etiam $\frac{\partial \log M}{\partial x}$ ipsam x involvit atque ψ non solius u vel Φ non solius $x-\xi$ functio est. Quoties autem $\Phi = \frac{\partial \log M}{\partial x}$ solius $x-\xi$ functio est, erit $\frac{\partial \Phi}{\partial x}$ ipsius Φ functio. Unde *e systematis propositi Multiplicatore cognito M semper deducere licet absque integratione systematis proprii unum plurave Integralia, quoties $\frac{\partial^2 \log M}{\partial x^2}$ non ipsius $\frac{\partial \log M}{\partial x}$ functio est.* Similiter demonstratur, *cognito systematis propositi Integrali, variabili x affecto, $v=\alpha$, designante α Constantem Arbitrariam, ex eo semper derivari posse unum plurave systematis proprii Integralia, nisi $\frac{\partial v}{\partial x}$ ipsius v functio sit.* Nam cum esse debeat v quantitatum $x-\xi$, f_1, f_2, ... f_{n-1} functio, ex aequatione $v=\alpha$ sequitur huiusmodi

$$x = \xi + \psi(\alpha, f_1, f_2, \dots f_{n-1});$$

unde eruendo e $v=\alpha$ ipsius x valore in eoque ponendo ipsius α loco varios valores constantes arbitrarios, differentiae expressionum provenientium Constantibus Arbitrariis aequiparatae suppeditabunt systematis proprii Integralia.

Ut habeatur exemplum quo systematis propositi Multiplicator variabili x affectus innotescit ideoque post systematis proprii integrationem completam ipsa x per $x_1, x_2, \dots x_n$ absque Quadratura exprimitur, ponamus $X=1$ simulque fieri

$$\frac{\partial X_1}{\partial x_1} + \frac{\partial X_2}{\partial x_2} \dots + \frac{\partial X_n}{\partial x_n} = c,$$

designante c quantitatem constantem; quod inter alia evenit, si X_1, X_2 etc. variabilium x_1, x_2 etc. functiones sunt lineares. Dabitur systematis propositi Multiplicator per formulam

$$\frac{d \log M}{dx} + c = 0, \text{ unde } M = e^{-cx}.$$

Hinc sequitur e (6.) sumendo logarithmos,

$$x = -\frac{1}{c} \log \left(\frac{1}{X_n} \Sigma \pm \frac{\partial f_1}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \dots \frac{\partial f_{n-1}}{\partial x_{n-1}} \right) + \text{Const.}$$

Cognitione igitur Multiplicatoris in hoc exemplo non reductionem aequationis differentialis ad Quadraturas sed Quadraturam lucramur.

Antecedentibus demonstratum est, *si aequationum differentialium* (1.), *in quibus X, X_1 etc. solarum $x_1, x_2, \dots x_n$ functiones sunt, detur Multiplicator et ipse variabili x vacans, duas postremas integrationes per Quadraturam absolvi; si Multiplicator variabili x afficiatur, ultimam aequationem integralem ipsam sine Quadratura obtineri.* Quae propositio sic amplificatur.

Ponamus functiones X_{m+1}, X_{m+2}, ... X_n vacuas esse a variabilibus x, x_1, ... x_m, simulque X, X_1, ... X_m nisi ab iisdem variabilibus vacuae sunt, certe satisfacere conditioni,

$$7. \quad \frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \dots + \frac{\partial X_m}{\partial x_m} = 0.$$

Eo casu aequationes differentiales propositae (1.) sic tractabuntur, ut primum aequationum differentialium inter solas x_{m+1}, x_{m+2}, ... x_n locum habentium,

$$8. \quad dx_{m+1} : dx_{m+2} \dots : dx_n = X_{m+1} : X_{m+2} \dots : X_n,$$

quaerantur Integralia,

$$9. \quad f_1 = \alpha_1, \quad f_2 = \alpha_2, \quad \dots \quad f_{n-m-1} = \alpha_{n-m-1},$$

eorumque ope exprimantur variabiles x_{m+1}, x_{m+2}, ... x_n per earum unam x_{m+1}; quibus factis superest ut integrentur aequationes differentiales inter ipsas x, x_1, ... x_{m+1} locum habentes,

$$10. \quad dx : dx_1 \dots : dx_{m+1} = X : X_1 \dots : X_{m+1}.$$

Per conditionem (7.) constat, aequationum differentialium propositarum (1.) Multiplicatorem, a variabilibus x, x_1, ... x_m vacuum, eundem esse aequationum differentialium (8.) Multiplicatorem, et vice versa harum Multiplicatorem ipsarum quoque aequationum differentialium (1.) Multiplicatorem esse. Designante enim M quantitatem a variabilibus x, x_1, ... x_m vacuam, sequitur e (7.),

$$\frac{\partial . MX}{\partial x} + \frac{\partial . MX_1}{\partial x_1} \dots + \frac{\partial . MX_m}{\partial x_m} = 0,$$

unde pro eiusmodi ipsius M valore conditio ut M aequationum (1.) sit Multiplicator,

$$\frac{\partial . MX}{\partial x} + \frac{\partial . MX_1}{\partial x_1} \dots + \frac{\partial . MX_n}{\partial x_n} = 0,$$

convenit cum conditione ut M aequationum (8.) Multiplicator sit,

$$\frac{\partial . MX_{m+1}}{\partial x_{m+1}} + \frac{\partial . MX_{m+2}}{\partial x_{m+2}} \dots + \frac{\partial . MX_n}{\partial x_n} = 0.$$

Aequationum differentialium (10.) *semper assignare licet Multiplicatorem.* Nam cum ipsarum x_{m+2}, x_{m+3}, ... x_n expressiones per x_{m+1} e (9.) petitae ab ipsis x, x_1, ... x_m vacuae sint, conditio (7.) valebit etiam post harum expressionum substitutionem. Qua substitutione cum X_{m+1} in solius x_{m+1} functionem abeat, valebit etiam aequatio (7.), si loco ipsarum X_i ponitur $\frac{X_i}{X_{m+1}}$. Unde sequitur, *aequationum differentialium* (10.) *Multiplicatorem esse* $\frac{1}{X_{m+1}}$. Qua de re *aequationum differentialium* (10.) *ultima integratio semper solis Quadraturis absolvitur.*

Si datur Multiplicator aequationum differentialium propositarum (1.), va-

riabilibus x, x_1, ... x_m non affectus, idem erit aequationum (8.) Multiplicator, ideoque eo casu cum aequationum (8.) tum aequationum (10.) ultima integratio Quadraturis absolvitur. Iam vero sit aequationum differentialium propositarum (1.) datus Multiplicator M variabilibus x, x_1, ... x_m affectus. Inventis aequationum differentialium (8.) Integralibus (9.), earum fit Multiplicator

$$N = \frac{1}{X_{m+1}} \Sigma \pm \frac{\partial f_1}{\partial x_{m+2}} \cdot \frac{\partial f_2}{\partial x_{m+3}} \cdots \frac{\partial f_{n-m-1}}{\partial x_n}$$

idemque ex antecedentibus fit Multiplicator aequationum differentialium propositarum (1.). Quarum igitur cognitis duobus Multiplicatoribus M et N, datur absque Quadratura Integrale

$$\frac{N}{M} = \frac{1}{MX_{m+1}} \Sigma \pm \frac{\partial f_1}{\partial x_{m+2}} \cdot \frac{\partial f_2}{\partial x_{m+3}} \cdots \frac{\partial f_{n-m-1}}{\partial x_n} = \text{Const.}$$

Quod substituendo ipsarum x_{m+2}, x_{m+3}, ... x_n valores per x_{m+1} exhibitos in aequationum (10.) Integrale abit. Harum aequationum praeterea vidimus ultimam integrationem Quadraturis absolvi. Unde propositis aequationibus differentialibus,

$$dx : dx_1 \ldots : dx_n = X : X_1 \ldots : X_n,$$

in quibus functiones X_{m+1}, X_{m+2}, ... X_n variabilibus x, x_1, ... x_m vacant simulque fit

$$\frac{\partial X}{\partial x} + \frac{\partial X_1}{\partial x_1} \cdots + \frac{\partial X_m}{\partial x_m} = 0,$$

si datur Multiplicator et ipse variabilibus x, x_1, ... x_m vacans, duae integrationes per Quadraturas absolvuntur; si vero datus Multiplicator variabilibus x, x_1, ... x_n afficitur, una aliqua aequatio integralis absque omni Quadratura constabit atque altera integratio Quadraturis efficietur.

Antecedentia exemplo esse possunt, ad aequationes differentiales integrandas e Multiplicatoris cognitione semper fructum aliquem percipi, etsi ultima integratio absque eius auxilio Quadraturis absolvi possit. Neque nessarium est ut in antecedentibus aequationes (4.) sint Integralia ipsarum aequationum differentialium (2.), vel aequationes (9.) sint Integralia ipsarum aequationum differentialium (8.). Nam secundum ea quae §. 12. tradidi, Constanti Arbitrariae post quamque novam integrationem accedenti valorem tribuere licet particularem quemcunque. Sufficit ut quaelibet aequatio f_i = Const. sit Integrale aequationum differentialium quocunque modo transformatarum per aequationes integrales ante eam inventas,

$$f_1 = \alpha_1, \quad f_2 = \alpha_2, \quad \ldots \quad f_{i-1} = \alpha_{i-1},$$

in quibus ad dextram habentur quantitates constantes quaecunque particulares.

17.

Beiträge zur Kreistheilung.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

I.

Es sei p eine positive ungerade Primzahl, r eine Wurzel der Gleichung

$$1.\quad \frac{x^p-1}{x-1}=0,$$

ω eine *primitive* Wurzel der Gleichung

$$2.\quad x^{p-1}=1$$

ist. Dies vorausgesetzt, kann man bekanntlich die ganze Theorie der *Kreistheilung* oder der Auflösung der Gleichung (1.) auf die Betrachtung der folgenden Reihen zurückführen:

$$3.\quad \varphi(\alpha,\beta)=\sum_{k=1}^{k=p-1}\omega^{\alpha\,\mathrm{Ind}.k}\,r^{\beta k},$$

mit denen wir uns hier beschäftigen wollen.

Wenn man die Werthe dieser Reihen für jeden ganzen Werth von α und β kennt, so läfst sich alles Übrige leicht daraus ableiten. Die Bestimmung der Perioden von $p$ten Wurzeln der Einheit, so wie die Auffindung der Wurzeln selbst, erfordert dann nur die Auflösung *linearer Systeme* von Gleichungen, bei welchen die Coëfficienten, also auch die Multiplicatoren, $p-1$te Wurzeln der Einheit sind. (*Gaufs disq. arith. Art.* 360.)

Man hat zunächst, wie aus dem blofsen Anblick der Reihen zu sehen,

$$4.\quad \varphi(\alpha,\beta)=\varphi(\alpha',\beta'),$$

wenn $\alpha\equiv\alpha'$ (mod. $p-1$) und $\beta\equiv\beta'$ (mod. p); ferner

$$5.\quad \varphi(\alpha,0)=0,$$

wenn α nicht durch $p-1$ theilbar ist und

$$6.\quad \varphi(0,\beta)=-1,$$

wenn β nicht durch p theilbar ist; dagegen

$$7.\quad \varphi(0,0)=p-1.$$

Hieraus folgt, dafs nur diejenigen Reihen zu betrachten nöthig sind, in welchen α und β die Werthe

$$\alpha=1,\ 2,\ 3,\ \ldots\ldots\ p-2,$$
$$\beta=1,\ 2,\ 3,\ \ldots\ldots\ p-1$$

haben. Die Relationen, welche zwischen diesen Reihen stattfinden, sind doppelter Art, je nachdem man α oder β sich ändern läfst.

Was zunächst die Functionen $\varphi(\alpha, \beta)$ betrifft, insofern man β als variabel ansieht, so behaupte ich, dafs sich eine solche Reihe immer auf die einfachere $\varphi(\alpha, 1)$ zurückführen läfst. In der That, wenn man $\beta k = k'$ setzt, so sind die Werthe, welche k' durchläuft, abgesehen von den Vielfachen von p, wieder die Glieder der Reihe

$$1, 2, 3, \ldots. p-1,$$

wenn auch in anderer Ordnung. Aus $\beta k = k'$ folgt nun

$$\text{Ind.}\,\beta + \text{Ind.}\,k \equiv \text{Ind.}\,k' \pmod{p-1},$$

also hat man

$$\sum_{k=1}^{k=p-1} \omega^{\alpha\,\text{Ind.}\,k}\, r^{\beta k} = \sum_{k'=1}^{k'=p-1} \omega^{\alpha\,\text{Ind.}\,k'}\, \omega^{-\alpha\,\text{Ind.}\,\beta}\, r^{k'},$$

folglich

$$8. \quad \varphi(\alpha, \beta) = \omega^{-\alpha\,\text{Ind.}\,\beta}\, \varphi(\alpha, 1).$$

Alle Reihen von der Form $\varphi(\alpha, \beta)$ reduciren sich demnach auf die folgenden $p-2$:

$$9. \quad \varphi(1, 1), \quad \varphi(2, 1), \quad \ldots. \quad \varphi(p-2, 1).$$

Wenn α ein Theiler von $p-1$ ist und man hat $p-1 = m\alpha$, so ist $\omega^{m\alpha} = 1$, folglich aus der Formel (8.), wenn man dem β nach und nach die Werthe

$$1, 2, 3, \ldots. m$$

giebt:

$$\varphi(\alpha, 1)\, \varphi(\alpha, 2) \ldots. \varphi(\alpha, m) = \varphi(\alpha, 1)^m = \varphi(\alpha, \beta)^m.$$

Da nun der Ausdruck links offenbar eine symmetrische Verbindung aller Wurzeln der Gleichung (1.) ist, so wird die Potenz $\varphi(\alpha, 1)^m$ eine blofse Function von ω^α sein, d. h. sie wird einem Ausdrucke von der Form

$$10. \quad A + B\omega^\alpha + C\omega^{2\alpha} + \ldots. + L\omega^{p-\alpha-1}$$

gleich sein, wo A, B, C etc. *reelle ganze Zahlen* vorstellen. Für den Werth von $\varphi(\alpha t, 1)^m$ wird sogleich hieraus gefunden:

$$11. \quad A + B\omega^{t\alpha} + C\omega^{2t\alpha} + \ldots + L\omega^{(p-\alpha-1)t}.$$

Wenn t zu $p-1$ relative Primzahl ist, so mufs man bis zur $p-1$ten Potenz von $\varphi(t, 1)$ aufsteigen, ehe man zu einem Ausdrucke von der Form (10.) gelangt.

Um neue Relationen zu erhalten, wollen wir die beiden Reihen $\varphi(\alpha, 1)$ und $\varphi(-\alpha, 1)$ mit einander multipliciren. Es ist

$$\varphi(\alpha, 1)\, \varphi(-\alpha, 1) = \sum_{k=1}^{k=p-1} \sum_{k'=1}^{k'=p-1} \omega^{\alpha(\text{Ind.}\,k - \text{Ind.}\,k')}\, r^{k+k'}.$$

Da hier für jeden stehenden Werth von k', k die Werthe $1, 2, \ldots. p-1$

durchlaufen soll, so kann man auch k durch $k'\sigma$ ersetzen, wenn man σ für jeden Werth von k' dieselben Werthe $1, 2, \ldots. p-1$ durchlaufen läfst. Wenn man noch bemerkt, dafs

$$\alpha(\text{Ind.}k'\sigma - \text{Ind.}k') = \alpha\,\text{Ind.}\sigma$$

ist, so zeigt sich, dafs die obige Doppelreihe durch diese Substitution in

$$\Sigma^{\sigma}\Sigma^{k'}\omega^{\alpha\,\text{Ind.}\sigma}\,r^{k'(\sigma+1)}$$

übergeht. Die Summation nach k' kann jetzt ausgeführt werden; man hat nämlich für jeden Werth von σ, mit Ausnahme des Werthes $\sigma = p-1$,

$$\sum_{k'=1}^{k'=p-1} r^{k'(\sigma+1)} = r + r^2 + \ldots. + r^{p-1} = -1;$$

dagegen für den Werth $\sigma = p-1$,

$$\sum_{k'=1}^{k'=p-1} r^{k'(\sigma+1)} = \sum_{k'=1}^{k'=p-1} r^{k'p} = p-1;$$

also wird der Werth der Doppelreihe:

$$-\omega^{\alpha\,\text{Ind.}1} - \omega^{\alpha\,\text{Ind.}2} - \text{etc.} - \omega^{\alpha\,\text{Ind.}(p-2)} + (p-1)\omega^{\alpha\,\text{Ind.}(p-1)}$$

$$= -(\omega^{\alpha} + \omega^{2\alpha} + \ldots. + \omega^{(p-1)\alpha}) + \omega^{\alpha\,\text{Ind.}(p-1)}p = \omega^{\alpha\,\text{Ind.}(p-1)}p = (-1)^{\alpha}p,$$

weil $\text{Ind.}(p-1) = \frac{1}{2}(p-1)$ und $\omega^{\frac{1}{2}(p-1)} = -1$ ist. Man hat daher das merkwürdige Resultat:

$$12. \quad \varphi(\alpha, 1)\,\varphi(-\alpha, 1) = (-1)^{\alpha}.p.$$

Wir wollen die Anwendbarkeit desselben durch ein Paar Beispiele nachweisen. Es sei zuerst $\alpha = \frac{1}{2}(p-1)$, also $\omega^{\alpha} = -1$. Da in diesem Fall $\alpha \equiv -\alpha \pmod{p-1}$, also $\varphi(\alpha, 1)\,\varphi(-\alpha, 1)$ ist, so geht (12.) in

$$\varphi(\tfrac{1}{2}(p-1), 1)^2 = (-1)^{\frac{1}{2}(p-1)}.p \text{ über, woraus}$$

$$\varphi(\tfrac{1}{2}(p-1), 1) = \sqrt{((-1)^{\frac{1}{2}(p-1)}.p)}, \text{ d. h.}$$

$$13. \quad \sum_{k=1}^{k=p-1}\left(\frac{k}{p}\right)r^k = \sqrt{((-1)^{\frac{1}{2}(p-1)}.p)} \text{ folgt;}$$

welches die bekannte Gaufsische Formel ist. Die Gleichung (8.) liefert hierzu noch

$$14. \quad \sum_{k=1}^{k=p-1}\left(\frac{k}{p}\right)r^{\beta k} = \left(\frac{\beta}{p}\right)\sqrt{((-1)^{\frac{1}{2}(p-1)}.p)}.$$

Das *Zeichen der Quadratwurzel* bleibt, wie zu vermuthen war, *unbestimmt,* und kann auch der Natur der Sache nach nicht durch die Kreistheilung selbst bestimmt werden. Alle andern Unbestimmtheiten können durch angemessene Betrachtungen leicht gehoben werden; aber diejenigen, welche die Wurzelzeichen hineinbringen, erfordern ganz besondere Untersuchungen, und ihre Beseitigung gehört zu den schwierigsten Problemen der Arithmetik. Für den in Rede stehenden Fall haben *Gaufs* und *Lejeune Dirichlet* die

Schwierigkeit durch höchst eigenthümliche und merkwürdige Betrachtungen überwunden, welche das bewunderungswürdige Genie dieser beiden berühmten Mathematiker ins hellste Licht setzen; aber ihre gleichsam auf diesen speciellen Fall berechneten Principien scheinen bei andern Fällen ihre Anwendbarkeit zu verlieren.

Zweitens sei für den Fall, dafs p von der Form $3m+1$ ist, $\alpha = \frac{1}{3}(p-1)$, so dafs ω^α eine imaginäre dritte Wurzel der Einheit wird, die wir durch ϱ bezeichnen wollen. In diesem Falle giebt die Formel (12.)

$$\varphi(\tfrac{1}{3}(p-1), 1)\,\varphi(\tfrac{2}{3}(p-1), 1) = p.$$

Nun lassen sich die dritten Potenzen der beiden Factoren auf der linken Seite auf die Form

$$\varphi(\tfrac{1}{3}(p-1), 1)^3 = A+B\varrho, \quad \varphi(\tfrac{2}{3}(p-1), 1)^3 = A+B\varrho^2$$

bringen, wo A und B reelle ganze Zahlen sind. Von der andern Seite weifs man, dafs die Zerlegungen von p^3 (als Norm betrachtet) in complexe ganze Zahlen, die aus dritten Wurzeln der Einheit bestehen, sich alle aus den Zerlegungen von p ableiten lassen. Wenn nämlich $p = p_1 p_2$, wo $p_1 = a+b\varrho$, $p_2 = a+b\varrho^2$ und a, b ganze Zahlen sind, so kann man nur setzen: entweder

$$p^3 = p_1^3 \times p_2^3, \text{ oder}$$
$$p^3 = pp_1 \times pp_2.$$

Da nun $\varphi(\frac{1}{3}(p-1), 1)$ selbst keine complexe ganze Zahl ist, so bleibt die erste Zerlegung ausgeschlossen und man hat also zu setzen:

$$A+B\varrho = pp_1, \quad A+B\varrho^2 = pp_2,$$

woraus

$$15. \quad \Sigma\varrho^{\text{Ind.}k} r^k = \sqrt[3]{(pp_1)}, \quad \Sigma\varrho^{2\text{Ind.}k} r^k = \sqrt[3]{(pp_2)}$$

folgt. Die Cubikwurzeln bleiben natürlich unbestimmt, aber man hat sie so zu wählen, dafs

$$\sqrt[3]{(pp_1)} : \sqrt[3]{(pp_2)} = p \text{ wird.}$$

Die Unbestimmtheit, welche dadurch entsteht, dafs man nicht weifs, welche von den zu derselben Gruppe gehörigen complexen Zahlen für p_1 zu nehmen sei, läfst sich leicht durch Betrachtungen beseitigen, von denen später die Rede sein wird.

Wir kehren jetzt wieder zu der allgemeinen Untersuchung zurück, und stellen uns die Aufgabe, den Werth des Productes

$$\varphi(\alpha, 1)\ \varphi(\beta, 1)$$

zu finden, wo vorausgesetzt wird, dafs weder α noch β, noch ihre Summe

$\alpha+\beta$ durch $p-1$ theilbar ist. Dieser Werth wird durch die Doppelreihe

$$\sum_{k=1}^{k=p-1}\sum_{k'=1}^{k'=p-1}\omega^{\alpha\,\mathrm{Ind.}\,k+\beta\,\mathrm{Ind.}\,k'}r^{k+k'} = S$$

gegeben. Ersetzen wir hier, wie oben, k durch $k'\sigma$, was erlaubt ist, weil für jeden stehenden Werth von k' die Reste der Vielfachen $k'\sigma$ nach dem mod. p mit den Werthen von k zusammenfallen, so kommt

$$S = \sum_{\sigma=1}^{\sigma=p-1}\sum_{k'=1}^{k'=p-1}\omega^{\alpha\,\mathrm{Ind.}\,k'+\alpha\,\mathrm{Ind.}\,\sigma+\beta\,\mathrm{Ind.}\,k'}r^{k'(\sigma+1)}$$

Um hier die Summation nach k' auszuführen, bedienen wir uns der beiden Formeln (5. und 8.). Die Formel (5.) zeigt, dafs für den Werth $\sigma=p-1$ die Summe nach k' verschwindet, weil sie

$$\varphi(\alpha+\beta,\ p) = \varphi(\alpha+\beta;\ 0)$$

wird. Für die übrigen Werthe von σ hat man

$\sum^{k'}\omega^{(\alpha+\beta)\,\mathrm{Ind.}\,k'}r^{(\sigma+1)k'} = \varphi(\alpha+\beta,\sigma+1) = \omega^{-(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)}\varphi(\alpha+\beta,1)$, nach (8.).

Man erhält also, da jetzt der Ausdruck $\varphi(\alpha+\beta,\ 1)$, der kein σ mehr enthält, als gemeinschaftlicher Factor aller Glieder heraustritt,

$$S = \sum_{\sigma=1}^{\sigma=p-2}\omega^{\alpha\,\mathrm{Ind.}\,\sigma-(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)}.\varphi(\alpha+\beta,\ 1).$$

Wir werden daher zu der neuen merkwürdigen Fundamentalformel geführt:

$$16.\qquad \frac{\varphi(\alpha,1)\varphi(\beta,1)}{\varphi(\alpha+\beta,1)} = \sum_{\sigma=1}^{\sigma=p-2}\omega^{\alpha\,\mathrm{Ind.}\,\sigma-(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)}.$$

Der Ausdruck auf der rechten Seite ist offenbar eine ***complexe ganze Zahl***, welche aus den Wurzeln ω zusammengesetzt ist; also ist der Ausdruck $\frac{\varphi(\alpha,1)\varphi(\beta,1)}{\varphi(\alpha+\beta,1)}$ immer einer complexen ganzen, aus $p-1$ten Wurzeln der Einheit zusammengesetzten Zahl gleich.

Wenn man die beiden Resultate (12. und 16.) verbindet, so erhält man

$$\frac{\varphi(\alpha,1)\varphi(\beta,1)}{\varphi(\alpha+\beta,1)}.\frac{\varphi(-\alpha,1)\varphi(-\beta,1)}{\varphi(-\alpha-\beta,1)} = \frac{(-1)^{\alpha}p.(-1)^{\beta}p}{(-1)^{\alpha+\beta}p} =$$
$$\sum_{\sigma=1}^{\sigma=p-2}\omega^{\alpha\,\mathrm{Ind.}\,\sigma-(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)}\times\sum\omega^{-\alpha\,\mathrm{Ind.}\,\sigma+(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)},$$

also

$$17.\qquad p = \sum_{\sigma=1}^{\sigma=p-2}.\omega^{\alpha\,\mathrm{Ind.}\,\sigma-(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)}\times\sum_{\sigma=1}^{\sigma=p-2}\omega^{-\alpha\,\mathrm{Ind.}\,\sigma+(\alpha+\beta)\,\mathrm{Ind.}\,(\sigma+1)}.$$

Man sieht hieraus, dafs, wenn m irgend ein Theiler von $p-1$ ist, die Primzahl p sich immer in das Product zweier complexen ganzen Zahlen mit

*m*ten Wurzeln der Einheit zerlegen läfst, die übrigens eine aus der andern hervorgehen, wenn man statt der Wurzel ihren reciproken Werth nimmt, so dafs die Primzahl p als die *Norm* einer jeden von beiden erscheint.

Durch eine specielle Anwendung dieser Formel auf die beiden Fälle, wo p eine Primzahl von der Form $4n+1$ oder $3n+1$ ist, erhält man, wenn man in beiden Fällen α und β durch n theilbar annimmt, die folgenden beiden interessanten Sätze.

Lehrsatz. „*Wenn p eine Primzahl von der Form* $4n+1$ *ist, i die Quadratwurzel* $\sqrt{-1}$ *bezeichnet, und man setzt*

$$\sum_{k=1}^{k=p-2} i^{\mathrm{Ind.}(k^2+k)} = A+Bi,$$

so ist

$$p = A^2+B^2."$$

Lehrsatz. „*Wenn p eine Primzahl von der Form* $3n+1$ *ist, ρ eine imaginäre Cubikwurzel der Einheit bezeichnet, und man setzt*

$$\sum_{k=1}^{k=p-2} \varrho^{\mathrm{Ind.}(k^2+k)} = A+B\varrho,$$

so ist

$$p = A^2-AB+B^2."$$

Man sieht, dafs durch diese Sätze nicht allein ein neuer Beweis für die Darstellbarkeit der Primzahl p durch die quadratischen Formen, resp. mit den Determinanten -1 und -3, gegeben ist, sondern dafs auch die *Werthe der Variabeln*, welche dieser Darstellung entsprechen und welche auf den ersten Blick als sehr complicirte numerische Transcendenten erscheinen, durch eine höchst einfache analytische Formel ausgedrückt werden, nach welcher man sie auch, wenn man will, mit grofser Leichtigkeit berechnen kann.

Für $p=13$ z. B. hat man

$$k = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12;$$

$$\mathrm{Ind.}k = 0,\ 5,\ 8,\ 10,\ 9,\ 1,\ 7,\ 3,\ 4,\ 2,\ 11,\ 6;$$

$$\mathrm{Ind.}(k^2+k) =$$

$$\mathrm{Ind.}k+\mathrm{Ind.}(k+1) = 5,\ 13,\ 18,\ 19,\ 10,\ 8,\ 10,\ 7,\ 6,\ 13,\ 17;$$

$$\mathrm{Ind.}k+\mathrm{Ind.}(k+1) \equiv 1,\ 1,\ 2,\ 3,\ 2,\ 0,\ 2,\ 3,\ 2,\ 1,\ 1 \pmod{4};$$

also

$$A+Bi = i^0+4i^1+4i^2+2i^3 = 1+4i-4-2i = -3+2i;$$

also ist

$$13 = 3^2+2^2 = 9+4; \text{ wie in der That.}$$

Die einmal berechneten Werthe von $\text{Ind.}k+\text{Ind.}(k+1)$ dienen nun auch gleichfalls, um die Zerlegung

$$13 = A^2 - AB + B^2$$

zu finden. Man mufs zu dem Ende, ebenso wie wir oben ihre Reste nach dem mod. 4 suchten, jetzt die Reste derselben Zahlen nach dem mod. 3 nehmen. Diese Reste sind

$$2,\ 1,\ 0,\ 1,\ 1,\ 2,\ 1,\ 1,\ 0,\ 1,\ 2;$$

folglich ist

$$A+B\varrho = 2+6\varrho+3\varrho^2 = -1+3\varrho, \quad 13 = 1+1.3+3^2.$$

Wenn $p-1 = m\alpha$ und $m > 2$ ist, so hindert nichts, in der Formel (17.) $\beta = -2\alpha$ zu setzen, weil für diesen Werth keine der drei Zahlen α, β, $\alpha+\beta$ durch $p-1$ theilbar ist. Die Formel wird dann, wenn man noch der Kürze wegen $\omega^\alpha = \zeta$ setzt, so dafs ζ eine *primitive* $m$te Wurzel der Einheit vorstellt,

$$18. \qquad p = \sum_{k=1}^{k=p-2} \zeta^{\text{Ind.}k+\text{Ind.}(k+1)} \times \sum_{k=1}^{k=p-2} \zeta^{-[\text{Ind.}k+\text{Ind.}(k+1)]}.$$

Hieraus zeigt sich, dafs man *alle* Zerlegungen einer vorgelegten Primzahl p in complexe ganze Zahlen durch einen *gemeinsamen Algorithmus* finden kann, wenn man ein für allemal für diese Primzahl die *Werthe* von $\text{Ind.}k+\text{Ind.}(k+1)$ berechnet; *durch diese Werthe* findet man nach und nach alle Zerfällungen, welche den verschiedenen Theilern m von $p-1$ entsprechen, wenn man die Reste dieser berechneten Werthe nach jedem einzelnen Theiler m sucht, und dann ganz einfach zählt, wie oft sich unter diesen Resten die Null, wie oft die Eins, die Zwei etc. befindet; die so gefundenen Anzahlen sind dann die Elemente der complexen ganzen Zahl mit $m$ten Wurzeln der Einheit. Auf diese Weise sind z. B. nach dem nachstehenden Schema die Zerfällungen der Primzahl $p = 61$ in das Product aus zwei complexen ganzen Zahlen mit 3ten, 4ten, 5ten und 12ten Wurzeln der Einheit berechnet. Man kann durch dasselbe Schema auch noch die Zerfällungen in complexe ganze Zahlen mit 15ten, 20ten und 60ten Wurzeln der Einheit, also alle überhaupt möglichen Zerfällungen finden. Durch ϱ, i, λ ist resp. eine dritte, vierte und fünfte primitive Wurzel der Einheit bezeichnet.

$p = 61$

k	Ind. k	Ind. k + Ind. $(k+1)$	Reste der Zahlen Ind. k + Ind. $(k+1)$ (mod. m)				k	Ind. k	Ind. k + Ind. $(k+1)$	Reste der Zahlen Ind. k + Ind. $(k+1)$ (mod. m)			
			$m=3$	$m=4$	$m=5$	$m=12$				$m=3$	$m=4$	$m=5$	$m=12$
1	0						31	59	88	1	0	3	4
2	1	1	1	1	1	1	32	5	64	1	0	4	4
3	6	7	1	3	2	7	33	21	26	2	2	1	2
4	2	8	2	0	3	8	34	48	69	0	1	4	9
5	22	24	0	0	4	0	35	11	59	2	3	4	11
6	7	29	2	1	4	5	36	14	25	1	1	0	1
7	49	56	2	0	1	8	37	39	53	2	1	3	5
8	3	52	1	0	2	4	38	27	66	0	2	1	6
9	12	15	0	3	0	3	39	46	73	1	1	3	1
10	23	35	2	3	0	11	40	25	71	2	3	1	11
11	15	38	2	2	3	2	41	54	79	1	3	4	7
12	8	23	2	3	3	11	42	56	110	2	2	0	2
13	40	48	0	0	3	0	43	43	99	0	3	4	3
14	50	90	0	2	0	6	44	17	60	0	0	0	0
15	28	78	0	2	3	6	45	34	51	0	3	1	3
16	4	32	2	0	2	8	46	58	92	2	0	2	8
17	47	51	0	3	1	3	47	20	78	0	2	3	6
18	13	60	0	0	0	0	48	10	30	0	2	0	6
19	26	39	0	3	4	3	49	38	48	0	0	3	0
20	24	50	2	2	0	2	50	45	83	2	3	3	11
21	55	79	1	3	4	7	51	53	98	2	2	3	2
22	16	71	2	3	1	11	52	42	95	2	3	0	11
23	57	73	1	1	3	1	53	33	75	0	3	0	3
24	9	66	0	2	1	6	54	19	52	1	0	2	4
25	44	53	2	1	3	5	55	37	56	2	0	1	8
26	41	85	1	1	0	1	56	52	89	2	1	4	5
27	18	59	2	3	4	11	57	32	84	0	0	4	0
28	51	69	0	1	4	9	58	36	68	2	0	3	8
29	35	86	2	2	1	2	59	31	67	1	3	2	7
30	29	64	1	0	4	4	60	30	61	1	1	1	1

Anzahl der Reste.

$m = 3$ { Reste 0, 1, 2 ; Anzahl 20, 15, 24 }, $m = 4$ { Reste 0, 1, 2, 3 ; Anzahl 17, 12, 12, 18 },

$m = 5$ { Reste 0, 1, 2, 3, 4 ; Anzahl 12, 12, 6, 15, 14 },

$m = 12$ { Reste 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 ; Anzahl 6, 6, 6, 6, 5, 4, 6, 4, 6, 2, 0, 8 }.

Also sind die complexen ganzen Zahlen

$$m = 3,\quad 20+15\varrho+24\varrho^2 = -4-9\varrho,$$
$$m = 4,\quad 17+12i-12-18i = 5-6i,$$
$$m = 5,\quad 12+12\lambda+6\lambda^2+15\lambda^3+14\lambda^4 = -6\lambda^2+3\lambda^3+2\lambda^4,$$
$$m = 12,\quad 6+6i\varrho+6i^2\varrho^2+6i^3\varrho^3+5i^4\varrho^4+4i^5\varrho^5+6i^6\varrho^6+4i^7\varrho^7+6i^8\varrho^8 \\ +2i^9\varrho^9+8i^{11}\varrho^{11} = \varrho(5+6i).$$

Wenn α ein Theiler von $p-1$ und $p-1 = m\alpha$ ist, so ist die $m$te Potenz von $\varphi(\alpha, 1)$ einer ganzen complexen Zahl mit $m$ten Wurzeln der Einheit gleich. Wir sind jetzt im Stande, diese ganze complexe Zahl *direct hinzuschreiben.* Es sei nämlich der Kürze halber allgemein

$$\varphi(\alpha, 1) = \psi(\alpha), \quad \sum_{k=1}^{k=p-2} \omega^{\alpha \,\text{Ind.}\, k - (\alpha+\beta)\,\text{Ind.}(k+1)} = S[\alpha, \beta];$$

dann nimmt die Gleichung (16.) folgende Gestalt an:

$$\psi(\alpha)\psi(\beta) = \psi(\alpha+\beta) S[\alpha, \beta],$$

für jeden Werth von α und β, wenn nur weder diese beiden Zahlen selbst, noch ihre Summe durch $p-1$ theilbar sind. Setzt man nun in diese Formel nach und nach

$$\beta = \alpha,\quad 2\alpha,\quad 3\alpha,\quad \ldots.\quad (n-1)\alpha,$$

multiplicirt alle so entstehenden Gleichungen mit einander und hebt auf beiden Seiten die gemeinschaftlichen Factoren fort, so erhält man

$$19.\quad \psi(\alpha)^n = S[\alpha, \alpha]\, S[\alpha, 2\alpha]\, S[\alpha, 3\alpha] \ldots.\, S[\alpha, (n-1)\alpha]\, \psi(n\alpha),$$

und diese Formel gilt, wenn *keine* der Zahlen

$$\alpha,\quad 2\alpha,\quad 3\alpha,\quad \ldots.\quad n\alpha \qquad (A.)$$

durch $p-1$ theilbar ist. Ist also namentlich α ein Theiler von $p-1$ und $p-1 = m\alpha$, so kann man $n = m-1$ nehmen und erhält dann aus der Verbindung von (19.) mit der oben bewiesenen Formel

$$\psi((m-1)\alpha)\psi(\alpha) = \psi(-\alpha)\psi(\alpha) = (-1)^\alpha p$$

die folgende:

$$\psi(\alpha)^m = (-1)^\alpha p\, S[\alpha, \alpha]\, S[\alpha, 2\alpha]\, S[\alpha, 3\alpha] \ldots.\, S[\alpha, (m-2)\alpha].$$

Setzt man daher $\omega^\alpha = \zeta$, so dafs ζ eine *primitive* $m$te Wurzel der Einheit wird, so hat man, wenn $p-1 = m\alpha$ ist,

$$20.\quad \psi(\alpha)^m = (-1)^\alpha p \sum \zeta^{\text{Ind.}k_1 - 2\,\text{Ind.}(k_1+1) + \text{Ind.}k_2 - 3\,\text{Ind.}(k_2+1) + \ldots. + \text{Ind.}k_{m-2} - (m-1)\,\text{Ind.}(k_{m-2}+1)} \\ = (-1)^\alpha p \sum \zeta^{\text{Ind.}[k_1 k_2 \ldots. k_{m-2}] - \text{Ind.}[(k_1+1)^2 (k_2+1)^3 \ldots. (k_{m-2}+1)^{m-1}]};$$

wo die Summation sich gleichzeitig über alle Werthe von $k_1, k_2, \ldots\ldots k_{m-2}$ aus der Reihe

$$1,\ 2,\ 3,\ \ldots\ldots\ p-2$$

erstreckt. Diese Formel ist merkwürdig, wenn man bedenkt, dafs durch dieselbe direct gegeben sind:

1. alle Werthe von $\psi(\alpha)$, also auch, wenn man ζ durch ζ^t ersetzt, alle Werthe von $\psi(\alpha t)$, wenn α Theiler von $p-1$ ist, also überhaupt die Werthe von $\varphi(\alpha, 1)$ für jeden Werth von α, mithin nach (8.) auch die Werthe der sämmtlichen Reihen $\varphi(\alpha, \beta)$. Also auch
2. alle Perioden von Wurzeln der Gleichung $\frac{x^p-1}{x-1} = 0$; folglich
3. die Auflösung aller Hülfsgleichungen und
4. die vollständige Auflösung der Gleichung (1.), wenn man, wie dies gewöhnlich geschieht, die der Gleichung $x^{p-1} = 1$ als bekannt voraussetzt.

Setzt man in der Formel (19.) $\alpha = 1$, so sieht man, dafs alle Reihen $\psi(n)$ sich durch die *einzige* $\psi(1)$ *rational*, d. h. nur mit Hülfe von $p-1$ten Wurzeln der Einheit ausdrücken lassen; also lassen sich überhaupt alle Reihen $\varphi(\alpha, \beta)$ durch die *einzige* $\varphi(1, 1)$ *rational* ausdrücken.

Den Ausdruck $\psi(1)$ findet man nun einfach wie folgt. Nach der Formel (20.) ist die Potenz $\psi(1)^{p-1}$ einer complexen ganzen Zahl mit $p-1$ten Wurzeln der Einheit gleich, die man leicht mit Hülfe der Tabelle für die Indices berechnen kann, und die wir durch T bezeichnen wollen. Ist nun

$$p-1 = a^\alpha b^\beta c^\gamma \ldots\ldots,$$

wo $a, b, c \ldots\ldots$ *verschiedene* Primzahlen bezeichnen, so kann man setzen:

$$\frac{1}{p-1} = \frac{m}{a^\alpha} + \frac{m'}{b^\beta} + \frac{m''}{c^\gamma} + \ldots\ldots \pm t,$$

und dann hat man

$$21. \qquad \psi(1) = \sqrt[a^\alpha]{T^m} \cdot \sqrt[b^\beta]{T^{m'}} \cdot \sqrt[c^\gamma]{T^{m''}} \ldots\ldots T^{\pm t};$$

wo $m, m', m'', \ldots\ldots t$ positive ganze Zahlen vorstellen.

Aufser den hier vorkommenden Wurzelgröfsen, unter deren verschiedenen Werthen man eine beliebige Wahl treffen kann, erscheinen also bei der ganzen Auflösung der Gleichung $\frac{x^p-1}{x-1}$ *keine neuen* Wurzelgröfsen; wodurch denn jede Unbestimmtheit verschwindet.

Berlin im Februar 1844.



18.

Notiz über einige Producten-Ausdrücke.

(Von Herrn Dr. *Stern* in Göttingen.)

(Auszug aus einem Briefe desselben an den Herausgeber dieses Journals.)

In dem dritten Supplemente zur Integralrechnung (Bd. 4. S. 146 d. deutsch. Übers.) findet ***Euler*** durch verwickelte Betrachtungen den Ausdruck

$$\sqrt{3} = \tfrac{2}{1}.\tfrac{4}{5}.\tfrac{8}{7}.\tfrac{10}{11}\ldots.$$

Eine andere Beweisführung ist mir nicht bekannt. Indessen ist dieser Ausdruck nebst vielen andern in einer Formel enthalten, deren Ableitung so leicht ist, dafs ich sie Ihnen nicht mittheilen würde, wenn sie nicht vielleicht in den Elementen eine passende Stelle fände.

Aus den bekannten Formeln

$$\sin\frac{2m\pi}{2n} = \frac{2m\pi}{2n}.\frac{2n-2m}{2n}.\frac{2n+2m}{2n}.\frac{4n-2m}{4n}.\frac{4n+2m}{4n}\ldots. \quad \text{und}$$

$$\sin\frac{m\pi}{2n} = \frac{m\pi}{2n}.\frac{2n-m}{2n}.\frac{2n+m}{2n}.\frac{4n-m}{4n}.\frac{4n+m}{4n}\ldots.$$

ergiebt sich nemlich sogleich, da

$$\sin\frac{2m\pi}{2n} = 2\sin\frac{m\pi}{2n}\cos\frac{m\pi}{2n}$$

ist, die Formel

$$\cos\frac{m\pi}{2n} = \frac{2n-2m}{2n-m}.\frac{2n+2m}{2n+m}.\frac{4n-2m}{4n-m}.\frac{4n+2m}{4n+m}\ldots.$$

Setzt man in dieser Formel $m=1$, $n=3$, so findet man, übereinstimmend mit ***Eulers*** Resultat,

$$\cos 30^0 = \frac{\sqrt{3}}{2} = \frac{4}{5}.\frac{8}{7}.\frac{10}{11}\ldots.$$

Setzt man $m=1$, $n=2$, so hat man die bekannte Formel

$$\cos 45^0 = \frac{\sqrt{2}}{2} = \frac{2}{3}.\frac{6}{5}.\frac{6}{7}.\frac{10}{9}\ldots.$$

Ebenso ergiebt sich, wenn man $m=2$, $n=5$ setzt,

$$\sqrt{5}+1 = \frac{4}{1}.\frac{6}{8}.\frac{14}{12}.\frac{16}{18}.\frac{24}{22}\ldots.$$

und so weiter.

Auch ergiebt sich daraus

$$\operatorname{tang}\frac{m\pi}{2n} = \frac{m\pi}{2n}\cdot\frac{2n-m}{2n}\cdot\frac{2n-m}{2n-2m}\cdot\frac{2n+m}{2n}\cdot\frac{2n+m}{2n+2m}\cdots,$$

woraus sich wieder viele Ausdrücke ableiten lassen. Setzt man z. B. $m=1$, $n=3$, so hat man

$$\log 30^0 = \frac{1}{\sqrt{3}} = \frac{\pi}{6}\cdot\frac{5}{6}\cdot\frac{5}{4}\cdot\frac{7}{6}\cdot\frac{7}{8}\cdot\frac{11}{12}\cdot\frac{11}{10}\cdot$$

Da auch

$$\sin\frac{m\pi}{2n} = \frac{m}{n}\cdot\frac{2n-m}{n}\cdot\frac{2n+m}{3n}\cdot\frac{4n-m}{3n}\cdots$$

ist, so hat man ferner

$$\operatorname{tang}\frac{m\pi}{2n} = \frac{m}{n}\cdot\frac{2n-m}{2n-2m}\cdot\frac{2n-m}{n}\cdot\frac{2n+m}{2n+2m}\cdot\frac{2n+m}{3n}\cdot\frac{4n-m}{4n-2m}\cdot\frac{4n-m}{3n}\cdots$$

Göttingen am 12ten März 1844.

19.
Aufgaben und Lehrsätze.

Théorèmes arithmétiques.

(Par Mr. *Gotth. Eisenstein* à Berlin.)

En désignant par $E(\Omega)$ *l'entier* immédiatement plus petit que Ω, j'ai trouvé les théorèmes suivants.

I. M et N étant deux *entiers* quelconques dont le second ne divise pas le premier, on aura

$$E\left(\frac{M}{N}\right) = \frac{M}{N} - \tfrac{1}{2} + \frac{1}{2N} \sum_{k=1}^{k=N-1} \sin\frac{2Mk\pi}{N} \cot\frac{k\pi}{N}.$$

II. Le *résidu minimum* de M pour le module N est égal à

$$\tfrac{1}{2}\left[N - \sum_{k=1}^{k=N-1} \sin\frac{2Mk\pi}{N} \cot\frac{k\pi}{N}\right].$$

III. M et N étant tous les deux *impairs et premiers entre eux,* on a

$$\sum_{k=1}^{k=\frac{1}{2}(N-1)} E\left(\frac{kM}{N}\right) = \frac{N^2-1}{8}\cdot\frac{M}{N} - \frac{N-1}{4} - \frac{1}{2N} \sum_{k=1}^{k=\frac{1}{2}(N-1)} \frac{\operatorname{tang}\frac{kM\pi}{N}}{\operatorname{tang}\frac{2k\pi}{N}}.$$

IV. p étant un nombre *premier*, a un nombre *impair* et non-divisible par p, on aura l'équation élégante:

$$\left(\frac{a}{p}\right) = (-1)^T, \text{ où } T = \frac{1}{2p}\left\{\frac{(a-2)p^2+2p-a}{4} - \sum_{k=1}^{k=\frac{1}{2}(p-1)} \frac{\operatorname{tang} k\frac{a\pi}{p}}{\operatorname{tang} k\frac{2\pi}{p}}\right\}.$$

V. M et N étant premiers entre eux et tous les deux $\equiv 1$ (mod. μ), on aura

$$\sum_{h=1}^{h=\frac{N-1}{\mu}} E\left(\frac{hM}{N}\right) + \sum_{h=1}^{h=\frac{M-1}{\mu}} E\left(\frac{hN}{M}\right) = \frac{(M-1)(N-1)}{\mu^2}.$$

keitsrechnung," von Dr. *L. Öttinger,* Freiburg i. Br. 1840, §. 1. Nr. 6. und §. 5. zu finden. Dort ist diese Aufgabe nur als die erste einer Reihe anderer, sich auf Polynome beziehender Aufgaben behandelt.

(Nachtrag des Herausgebers d. Journ. zu der Aufgabe.)

In dem Abdruck derselben befindet sich ein *Druckfehler,* und zwar *ersichtlicherweise;* denn was da steht, giebt keinen bestimmten Sinn. Vor dem Worte „Glieder" fehlen nemlich zweimal, in Z. 6 und Z. 12 v. u., die Worte „nach den a verschiedenen." Der *so* vollständig ausgedrückte Satz, dafs *die Anzahl der sämmtlichen, nach den a verschiedenen Gliedern der Entwicklung von* $(a_0+a_1x+a_2x^2\ldots.+a_nx^n)^m$ *mit gleichen oder ungleichen Potenzen von* x *allgemein durch den Binomial-Coëfficienten* $(m+n)_n$ *oder* $(m+n)_m$ ausgedrückt wird, ist dann richtig. Z. B. es ist für $n=2$, $m=4$:

$$(a_0+a_1x+a_2x^2)^4 = a_0^4+4a_1a_0x+\left.\begin{matrix}6a_0^2a_1^2\\+4a_2a_0^3\end{matrix}\right\}x^2+\left.\begin{matrix}4a_0a_1^3\\+12a_1a_2a_0^2\end{matrix}\right\}x^3+\left.\begin{matrix}a_1^4\\+6a_0^2a_2^2\\+12a_0a_2a_1^2\end{matrix}\right\}x^4$$
$$+\left.\begin{matrix}4a_2a_1^3\\+12a_0a_1a_0^2\end{matrix}\right\}x^5+\left.\begin{matrix}4a_0a_2^3\\+6a_1^2a_2^2\end{matrix}\right\}x^6+4a_1a_2^3x^7+a_2^4x^8;$$

und hier ist die Anzahl der sämmtlichen nach den a verschiedenen Glieder mit gleichen und ungleichen Potenzen von x, $=1+1+2+2+3+2+2+1+1$ $=15=6_2=(m+n)_m$. Der Satz ist auch *bekannt,* wie es die Aufgabe bemerkt. Er findet sich z. B. in einer Abhandlung von *Brianchon* im 25ten Heft des *Journal de l'école polytechnique.*

Druckfehler im 26ten Bande.

S. 89 Z. 13 v. o. lese man $\log(1+A_1u\ldots.)$ statt $\tang(1+A_1u\ldots.)$

Im 27ten Bande.

S. 106 Z. 12 v. o. ist vor $a\Delta^2$, $b\Delta^2$, $c\Delta^2$, $d\Delta^2$ das Zeichen — zu setzen.

Fac-simile …

…tion

Monsieur

je suis très flatté des expressions bien

que vous nous avez transmis. les te…

seront confiés à ceux qui ont app…

il me sera toujours très agréable d…

par les communications que peuvent…

traitant la ville de paris à vous … important

utiles aux intérêts des sciences. j…

le secrétaire de l'institut un moye…

je suis présentement occupé de…

en suite je traiterai de nouveau que…

qui se rapportent au système du mo…

lors que le [illegible] vous

[illegible] revenir.

je m'estimerai toujours très honoré

de bruxelles. le choix de cette illus…

agréez monsieur…

…ieur Quetelet de l'académie…

lienen
nmter
n und
r un-
oder
plica-
Index
e zu-
hrens
x:
l ne-
dieser
raden

keitsr
§. 5.
sich

ersic
dem
Wort
dafs
Entw
Pote
(m +
(a_0 +

und
mit g
= 1
beme
Heft

S

S

20.

Elementare Ableitung einer merkwürdigen Relation zwischen zwei ungleichen Producten.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

Das fruchtbare Princip, dessen man sich in der Integralrechnung zu bedienen pflegt, um mit Hülfe von Doppel-Integralen die Werthe einfacher bestimmter Integrale zu finden, läfst sich auch mit Erfolg auf die Theorie der Reihen und der unendlichen Producte anwenden. Um Relationen zwischen Reihen oder unendlichen Producten zu erhalten, kann man von unendlichen Doppelreihen oder unendlichen Doppelproducten ausgehen und die Summation oder die Multiplication abwechselnd zuerst nach dem einen und dann nach dem andern Index ausführen. Man gelangt durch dieses Mittel auf ganz elementarem Wege zuweilen zu sehr merkwürdigen Resultaten.

Ein Beispiel statt aller wird genügen, um den Geist dieses Verfahrens anschaulich zu machen.

Es ist bekanntlich für jeden reellen und imaginären Werth von x:

$$\Pi\left(1-\frac{x}{\mu}\right)=\tfrac{1}{2}\left(e^{\frac{1}{2}(x\pi i)}+e^{-\frac{1}{2}(x\pi i)}\right),$$

wenn man die Multiplication auf der linken Seite über alle positiven und negativen *ungeraden* Werthe des Index μ ausdehnt. Schreibt man in dieser Formel $\frac{z-q}{p}$ statt x und bemerkt, dafs

$$1-\frac{z-q}{p\mu}=\left(1+\frac{q}{p\mu}\right)\left(1-\frac{z}{p\mu+q}\right)$$

ist, so erhält man

$$\Pi\left(1-\frac{q}{p\mu}\right)\Pi\left(1-\frac{z}{p\mu+q}\right)=\tfrac{1}{2}\left(e^{\frac{z-q}{2p}\pi i}+e^{\frac{q-z}{2p}\pi i}\right),$$

folglich

$$1.\quad \Pi\left(1-\frac{z}{p\mu+q}\right)=\frac{e^{\frac{z-q}{2p}\pi i}+e^{\frac{q-z}{2p}\pi i}}{e^{-\frac{q\pi i}{2p}}+e^{+\frac{q\pi i}{2p}}}.$$

Man nehme jetzt das unendliche Doppelproduct

$$2.\quad \Pi\left(1-\frac{z}{\mu A+\mu' A'}\right),$$

in welchem sich die Multiplication über alle positiven und negativen *ungeraden*

Werthe der beiden Indices μ und μ' erstrecken soll. Die beiden Constanten A und A' können beliebig complex gewählt werden, jedoch mit der Beschränkung, dafs der imaginäre Theil $\frac{A'}{A}$ nicht verschwinden darf. Diese Beschränkung ist nothwendig, weil im entgegengesetzten Falle das unendliche Doppelproduct nicht convergiren würde; wovon man sich leicht überzeugt, wenn man erwägt, dafs der analytische Modul des Ausdrucks

$$\mu A+\mu' A' = A\left(\mu+\mu\frac{A'}{A}\right)$$

jeden Grad der Kleinheit erreichen kann, wenn der imaginäre Theil von $\frac{A'}{A}$ verschwindet, oder dafs derselbe doch wenigstens einem bestimmten Ausdrucke für unendlich viele Werthe von μ und μ' gleich werden kann, im Fall $\frac{A'}{A}$ einen *rationalen* Werth haben sollte; dafs dagegen dieser Modul für einen von Null verschiedenen Werth des Quotienten $\frac{A'}{A}$ einmal immer über einer gewissen von Null verschiedenen Grenze liegt, also ein positives Minimum hat, und ferner auch unter jeder beliebigen gröfseren Grenze nur für eine endliche Anzahl von Werthen der Indices liegen kann.

Dieses vorausgesetzt, kann man jetzt die Multiplication in dem Producte (2.) nach dem einen Index μ verrichten, indem man in der Formel (1.) $p=A$, $q=\mu' A'$ setzt. Dadurch geht das unendliche Doppelproduct (2.) in ein einfaches Product über, dessen allgemeiner Factor die Form

$$\frac{e^{\frac{z-\mu'A'}{2A}\pi i}+e^{\frac{\mu'A'-z}{2A}\pi i}}{e^{-\frac{\mu'A'\pi i}{2A}}+e^{\frac{\mu'A'\pi i}{2A}}}$$

erhält. In diesem Ausdrucke mufs μ' alle positiven und negativen ungeraden Werthe erhalten; wir wollen daher diejenigen Werthe desselben wirklich mit einander multipliciren, welche entgegengesetzten Werthen des Index entsprechen. Dadurch verwandelt sich der allgemeine Factor in den folgenden:

$$\frac{1+\left(e^{\frac{z\pi i}{A}}+e^{-\frac{z\pi i}{A}}\right)e^{\frac{\mu'A'\pi i}{A}}+e^{\frac{2\mu'A'\pi i}{A}}}{\left(1+e^{\frac{\mu'A'\pi i}{A}}\right)^2},$$

wo aber μ' nur positive Werthe bekommen darf. Das unendliche Doppelproduct (2.) findet sich also auf folgende Weise ausgedrückt:

$$3.\quad \Pi\frac{1+\left(h^2+\frac{1}{h^2}\right)k^{\mu'}+k^{2\mu'}}{(1+k^{\mu'})^2},$$

wo der Kürze wegen $h = e^{\frac{z\pi i}{2A}}$, $k = e^{\frac{A'\pi i}{A}}$ gesetzt ist, und wo das Multiplicationszeichen sich auf alle positiven und ungeraden Werthe von μ' bezieht.

Geht man nun wieder von dem unendlichen Doppelproducte (2.) aus, verrichtet aber die Multiplication nach dem Index μ', so wird man, wie es sich auch schon aus dem symmetrischen Verhalten des Products in Beziehung auf die beiden Constanten A und A' schliefsen läfst, auf ein ganz ähnliches Resultat (3.) geführt; nur mit dem Unterschiede, dafs A und A' mit einander vertauscht erscheinen. Wir haben demnach die folgende merkwürdige Relation zwischen zwei unendlichen Producten:

$$4. \quad \Pi\left\{\frac{1+\left(h^2+\frac{1}{h^2}\right)k^{\mu}+k^{2\mu}}{(1+k^{\mu})^2}\right\} = \Pi\left\{\frac{1+\left(h'^2+\frac{1}{h'^2}\right)k'^{\mu}+k'^{2\mu}}{(1+k'^{\mu})^2}\right\},$$

wo der Kürze wegen

$$h = e^{\frac{z\pi i}{2A}}, \quad h' = e^{\frac{z\pi i}{2A'}},$$
$$k = e^{\frac{A'\pi i}{A}}, \quad k' = e^{\frac{A\pi i}{A'}}$$

gesetzt worden ist, und wo die beiden Multiplicationen links und rechts sich auf alle *positiven ungeraden* Werthe von μ beziehen.

Man kann auf ähnliche Weise auch von den beiden unendlichen Doppelproducten

$$5. \quad z\,\Pi\left(1-\frac{z}{\lambda A+\lambda' A'}\right) \quad \text{und} \quad \Pi\left(1-\frac{z}{\lambda A+\mu A'}\right)$$

ausgehen, wo die beiden Indices λ und λ' alle geraden Zahlen $0, \pm 2, \pm 4$ etc. repräsentiren, während μ die Werthe $\pm 1, \pm 3, \pm 5$ etc. durchläuft; wo jedoch bei dem ersten dieser beiden Producte die Combination $\lambda = 0$, $\lambda' = 0$ ausgeschlossen bleibt. Da die Rechnung der obigen für das Product (2.) sehr ähnlich ist, so wird es genügen, die Resultate hinzuschreiben. Man erhält

$$6. \quad A\left(h-\frac{1}{h}\right)\Pi\left\{\frac{1-\left(h^2+\frac{1}{h^2}\right)k^{\lambda}+k^{2\lambda}}{(1-k^{\lambda})^2}\right\}$$
$$= A'\left(h'-\frac{1}{h'}\right)\Pi\left\{\frac{1-\left(h'^2+\frac{1}{h'^2}\right)k'^{\lambda}+k'^{2\lambda}}{(1-k'^{\lambda})^2}\right\},$$

$$7. \quad \Pi\left\{\frac{1-\left(h^2+\frac{1}{h^2}\right)k^{\mu}+k^{2\mu}}{(1-k^{\mu})^2}\right\} = \tfrac{1}{2}\left(h'+\frac{1}{h'}\right)\Pi\left\{\frac{1+\left(h'^2+\frac{1}{h'^2}\right)k'^{\lambda}+k'^{2\lambda}}{(1+k'^{\lambda})^2}\right\}$$

37 *

Die Buchstaben h, h', k, k' bezeichnen hier genau Dasselbe wie in der Gleichung (4.) und λ und μ erhalten die Werthe

$$\lambda = 2, 4, 6 \text{ etc.}; \quad \mu = 1, 3, 5 \text{ etc.}$$

Durch einfache Division der in (2. und 5.) aufgestellten Producte erhält man die *elliptischen Functionen*. Die Betrachtung dieser unendlichen Doppelproducte scheint um so wichtiger, weil sich aus ihnen unmittelbar die doppelte Periodicität der elliptischen Functionen, so wie die Werthe der Variabeln ergeben, für welche die letztern verschwinden oder unendlich grofs werden, so dafs man hier ein vollständiges Bild von dem Gange dieser wichtigen Functionen erhält. Überhaupt scheinen die unendlichen Producte den Character einer Function besser auszusprechen, als jede andere Entwicklung.

Die hier angestellte Untersuchung ist übrigens so elementarer Natur, dafs sie sich wohl eignen möchte, den Anfänger in die Theorie der elliptischen Functionen einzuführen.

Berlin am 10ten Februar 1844.

21.

Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

Das Reciprocitätsgesetz für die quadratischen Reste, dessen strenger Beweis trotz der Bemühungen der ausgezeichnetesten Mathematiker früherer Zeit bis auf *Gaufs* vergeblich gesucht worden war, ist von dem berühmten Verfasser der *Disquisitiones arithmeticae* auf *sechs* von einander gänzlich verschiedene Arten bewiesen worden. Diese sechs Beweise, von denen jeder ein unschätzbares Kleinod genannt zu werden verdient, und ihre Principien liegen nun als ebenso viele Muster vor, um auf Untersuchungen höherer Art angewendet zu werden. Die Betrachtungen dieses unübertreflichen und in seiner hohen Genialität so einzig dastehenden Mathematikers sind aber so überaus eigenthümlicher und delicater Natur, dafs selbst das blofse Studium derselben nur einer geringen Zahl Bevorzugter vergönnt zu sein scheint, während die weitere Verfolgung und Benutzung seiner Gedanken mit den gröfsten Schwierigkeiten verknüpft ist. Dessenungeachtet lassen sich die in diesen Beweisen niedergelegten Principien ohne Zweifel auch auf schwierigere analoge Untersuchungen anwenden, und dies ist ja eben das unverkennbare Zeichen des Genies, dafs es auf den Wegen, welche es einschlägt, nicht allein unfehlbar das vorgesetzte Ziel erreicht, sondern auch zugleich die Mittel zur Besiegung gröfserer Schwierigkeiten vorbereitet. Indem wir den letzten und merkwürdigsten Beweis des grofsen Meisters einer aufmerksamen Betrachtung unterwarfen und den Ideengang verfolgten, durch welchen der Verfasser auf denselben geführt worden sein dürfte, bemerkten wir, dafs aus einer ähnlichen, aber viel näher liegenden Quelle, eine Reihe sehr allgemeiner Sätze geschöpft werden könne, welche für die Reste der höheren Potenzen dieselbe Stelle ausfüllen, die das bekannte Reciprocitätsgesetz in Beziehung auf die quadratischen Reste einnimmt.

Wir beschränken unsere Untersuchung in der gegenwärtigen Abhandlung auf die cubischen Reste, und werden besonders den schönen Reciprocitätssatz beweisen; welchen Hr. Professor *Jacobi* mitgetheilt hat, von welchem aber,

so viel ich weiſs, noch Niemand einen Beweis zu geben versucht hat. Da sich demnach hier zum ersten Male allgemeinere Sätze über die Reste der höheren Potenzen und über die Theiler der Ausdrücke höherer Ordnung nicht auf dem Wege der Induction, sondern auf dem der strengen Entwicklung abgeleitet finden, so wagen wir zu hoffen, daſs diese Abhandlung für die Zahlentheoretiker von einigem Interesse sein werde.

Die Elementarsätze der Theorie der ganzen *complexen* Zahlen von der Form

$$a+b\varrho,$$

wo ϱ eine imaginäre *Cubicwurzel* der Einheit bezeichnet, finden sich zwar noch nirgends aufgezeichnet; indessen glauben wir, wegen der groſsen Analogie, welche zwischen diesen complexen Zahlen und den gewöhnlich sogenannten complexen Zahlen von der Form

$$a+b\sqrt{(-1)}$$

herrscht, diese Sätze, in so weit sie sich auf Theilbarkeit der Zahlen durcheinander, Zerlegbarkeit in einfache Factoren, Theorie der complexen Primzahlen u. s. w. beziehen, hier als bekannt voraussetzen zu dürfen *). Man vergleiche übrigens die zweite Abhandlung von *Gauſs* über die biquadratischen Reste im 7ten Bande der *Commentationes Goettingenses rec.*, so wie die ersten 5 Paragraphen von *Dirichlet's Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes*, im 24sten Bande dieses Journals. Einige weniger einfache Betrachtungen, welche sich speciell auf die Theorie der cubischen Reste beziehen, haben wir in aller Kürze im zweiten Paragraph entwickelt.

---

§. 1.

Wir schicken unserer Untersuchung die folgenden Hülfssätze voraus.

Hülfssätze.

1. „Wenn p eine ungerade (reelle) Primzahl, r eine imaginäre $p$te Wurzel der Einheit ist, und man hat eine Gleichung von der Form

$$A+Br+Cr^2+\ldots\ldots+Mr^{p-2}=0,$$

wo $A, B, C, \ldots M$ *rationale* Zahlen sind, so ist nothwendig

$$A=B=C=\ldots\ldots=M=0.\text{"}$$

---

*) Der Mangel eines vollständigen Compendiums der *Zahlentheorie* wird hier recht fühlbar.

Denn fänden diese letzteren Gleichungen nicht statt, so wäre nicht *identisch* für jeden Werth von x

$$A+Bx+Cx^2+\ldots\ldots+Mx^{p-2}=0,$$

sondern es wäre $x=r$ eine Wurzel dieser Gleichung. Bezeichnen wir das erste Glied dieser Gleichung durch Φ, so hätten also die beiden Gleichungen

$$\Phi=0 \quad \text{und} \quad \frac{x^p-1}{x-1}=X=0$$

wenigstens eine gemeinschaftliche Wurzel. Sucht man auf die gewöhnliche Weise den gröfsten gemeinschaftlichen Theiler Ψ der beiden Polynome Φ und X, so müssen, wie aus der Art der Operation selbst erhellt, die Coëfficienten von ψ nothwendig rational sein. Es hätte also X einen rationalen Theiler Ψ; was ungereimt ist (*Disquisitiones Arithm. Art. 341.*).

2. „Wenn eine ganze Function der $p$ten Wurzeln der Einheit mit ganzen Coëfficienten einer *rationalen* Zahl μ gleich ist, so ist μ nothwendig eine *ganze* Zahl."

Jede ganze Function von der angegebenen Art läfst sich mit Hülfe des *Newton*schen Satzes und der Gleichung $1+r+r^2+\ldots\ldots+r^{p-1}=0$ auf die Form

$$a+br+cr^2+\ldots\ldots+mr^{p-2}=\mu$$

bringen, wo $a, b, c, \ldots\ldots m$ *ganze* Zahlen sind; ist nun μ rational, so schliefst man aus

$$a-\mu+br+cr^2+\ldots\ldots+mr^{p-2}=0$$

nach dem vorigen Satze

$$a-\mu=0, \quad b=0 \text{ etc.}:$$

also ist μ der ganzen Zahl a gleich; was zu beweisen war.

Derselbe Satz läfst sich auch auf complexe Zahlen von der Form $a+b\varrho$ ausdehnen, wenn ϱ eine imaginäre Cubikwurzel der Einheit vorstellt; in folgender Weise.

3. „Wenn eine ganze Function der $p$ten Wurzeln der Einheit mit ganzen complexen Coëfficienten der rationalen complexen Zahl $\mu+\nu\varrho$ gleich ist, und diese Gleichheit für beide Werthe der Cubikwurzel stattfindet, so ist nothwendig $\mu+\nu\varrho$ eine ganze complexe Zahl."

Denn bringt man die ganze Function auf die Form

$$a+a'\varrho+(b+b'\varrho)r+(c+c'\varrho)r^2+\ldots\ldots+(m+m'\varrho)r^{p-2},$$

wo a, a', b, b' etc. ganze Zahlen sind, und setzt

$$a+br+cr^2+\ldots\ldots+mr^{p-2}=U,$$
$$a'+b'r+c'r^2+\ldots\ldots+m'r^{p-2}=V,$$

so hat man nach der Annahme,

$$U+V\varrho = \mu+\nu\varrho, \quad U+V\varrho^2 = \mu+\nu\varrho^2,$$

also, wenn man addirt und subtrahirt,

$$2U-V=2\mu-\nu, \quad V=\nu, \quad \text{also auch} \quad U=\mu;$$

demnach sind, zufolge des vorigen Satzes, μ und ν ganze Zahlen.

Sind also α und β zwei ganze complexe Zahlen von der Form $a+b\varrho$, und ist ferner W eine ganze Function der $p$ten Wurzeln der Einheit mit ganzen complexen Coëfficienten, so schliefst man aus einer Gleichung von der Form

$$\alpha W = \beta,$$

wenn sie unabhängig von der Wahl der Cubikwurzel ϱ gilt, dafs nothwendig β durch α *theilbar* sein mufs. Dieser Satz läfst sich auch wie folgt aussprechen.

4. „Wenn der Werth einer ganzen Function der $p$ten Wurzeln der Einheit, deren Coëfficienten ganze complexe Zahlen und sämmtlich durch die ganze complexe Zahl α theilbar sind, der ganzen complexen Zahl β gleich ist, so findet die Congruenz

$$\beta \equiv 0 \pmod{\alpha} \text{ Statt.“}$$

Die Anwendung dieses Satzes ist für das Folgende von besonderer Wichtigkeit.

Aufser diesen einfachen Sätzen bedürfen wir noch der folgenden beiden.

5. „Wenn p eine reelle ungerade Primzahl vorstellt, so ist für jede *nicht* durch $p-1$ theilbare Zahl m die Summe der Potenzen

$$\sum_{\sigma=1}^{\sigma=p-1} \sigma^m \equiv 0 \pmod{p};$$

dagegen ist dieselbe Summe $\equiv -1 \pmod{p}$, wenn m durch $p-1$ theilbar ist.“

Die zweite Behauptung ist durch sich selbst klar, weil man für alle Werthe von σ, auf welche die Summation sich bezieht, $\sigma^{p-1} \equiv 1 \pmod{p}$ hat, folglich auch für jede ganze Zahl μ, $\sigma^{\mu(p-1)} \equiv 1$, mithin

$$\sum_{\sigma=1}^{\sigma=p-1} \sigma^{\mu(p-1)} \equiv p-1 \equiv -1 \pmod{p} \text{ ist.}$$

Wenn aber m nicht durch $p-1$ theilbar ist, so bezeichne man durch g irgend eine primitive Congruenzwurzel für den mod. p, und durch T den Werth der in Rede stehenden Summe; dann ist offenbar, wegen $\sigma \equiv g^{\text{Ind.}\sigma}$,

$$T \equiv \sum_{\sigma=1}^{\sigma=p-1} g^{m\,\text{Ind.}\sigma} \pmod{p}.$$

Ind. σ durchläuft, wenn auch in anderer Ordnung, die Werthe

$$0,\ 1,\ 2,\ 3,\ \ldots\ldots\ p-2;$$

also hat man

$$\sum_{\sigma=1}^{\sigma=p-1} g^{m\,\text{Ind.}\,\sigma} = \sum_{k=0}^{k=p-2} g^{mk} = \frac{1-g^{m(p-1)}}{1-g^m};$$

folglich ist

$$T \equiv \frac{1-g^{m(p-1)}}{1-g^m} \pmod{p} \text{ und}$$

$$(1-g^m)\,T \equiv 1-g^{m(p-1)} \pmod{p}.$$

Die rechte Seite dieser Congruenz ist durch p theilbar, wegen $g^{m(p-1)} \equiv 1 \pmod{p}$. Da nun m nicht durch $p-1$, also $1-g^m$ nicht durch p theilbar ist, so ist nothwendig

$$T \equiv 0 \pmod{p}.$$

Namentlich ist also für jede ganze Zahl m, von 1 bis $p-2$:

$$\sum_{\sigma=1}^{\sigma=p-2} \sigma^m \equiv -(p-1)^m \equiv (-1)^{m+1} \pmod{p}.$$

6. „Sind m und n zwei ganze Zahlen $<p-1$ und >0, so ist die Summe

$$\sum_{\sigma=1}^{\sigma=p-2} \sigma^m(\sigma+1)^n \equiv 0 \pmod{p},$$

wenn $m+n<p-1$ ist; dagegen

$$\sum_{\sigma=1}^{\sigma=p-2} \sigma^m(\sigma+1)^n \equiv -\frac{n!}{(m+n-p+1)!\,(p-1-m)!} \pmod{p},$$

wenn $m+n=p-1$ oder $m+n>p-1$ ist."

Entwickelt man das allgemeine Glied der Reihe nach dem binomischen Lehrsatze und setzt

$$\sigma^m(\sigma+1)^n = \sigma^{m+n} + n_1\sigma^{m+n-1} + n_2\sigma^{m+n-2} + \text{ etc.},$$

wo

n_1, n_2 etc. die Binomialcoefficienten

n, $\frac{1}{2}(n(n-1))$ vorstellen,

so erhält man die Doppelreihe

$$\sum_{\sigma=1}^{\sigma=p-2} \sum_{\tau=0}^{\tau=n} n_\tau\, \sigma^{m+n-\tau}.$$

In dieser Doppelreihe wollen wir zuerst die Summation betrachten, welche sich auf σ bezieht. Wenn $m+n<p-1$ ist, so sind alle Exponenten $m+n-\tau<p-1$, aber >0; folglich hat man in diesem Falle nach dem

5ten Hülfssatze für jeden stehenden Werth von τ:

$$\sum_{\sigma=1}^{\sigma=p-2} \sigma^{m+n-\tau} \equiv -(p-1)^{m+n-\tau} \pmod p.$$

Ist dagegen $m+n \geqq p-1$, so existirt ein und nur ein Werth von τ, für welchen $m+n-\tau$ durch $p-1$ theilbar ist, nemlich der Werth $m+n-p+1$. Für diesen besondern Werth von τ mufs also die obige Congruenz, welche für die übrigen Werthe von τ auch in diesem zweiten Falle richtig bleibt, durch die folgende ersetzt werden:

$$\sum_{\sigma=1}^{\sigma=p-2} \sigma^{m+n-\tau} \equiv -(p-1)^{m+n-\tau} - 1 \pmod{p}.$$

Es geht daher der Werth unserer Doppelreihe nach Abwerfung der Vielfachen von p in

$$-\sum_{\tau=0}^{\tau=n} n_\tau (p-1)^{m+n-\tau}$$

oder in

$$-\sum_{\tau=0}^{\tau=n} n_\tau (p-1)^{m+n-\tau} - n_{m+n-p+1}$$

über, je nachdem $m+n < p-1$ oder $m+n \geqq p-1$ ist.

Nun ist wieder nach dem binomischen Lehrsatze:

$$\sum_{\tau=0}^{\tau=n} n_\tau (p-1)^{m+n-\tau} = (p-1)^m p^n,$$

also durch p theilbar. Die Reihe, um deren Werth es sich handelt, wird daher je nach den beiden Fällen

$$\equiv 0 \quad \text{oder} \quad \equiv -n_{m+n-p+1}, \quad \text{w. z. b. w.}$$

§. 2.

Für jede gegebene ganze complexe Zahl $a+b\varrho = l$, als Modul, kann man die Gesammtheit aller ganzen complexen Zahlen in Partialreihen theilen: nach dem Princip, dafs man je zwei complexe Zahlen in dieselbe Reihe aufnimmt; oder in verschiedene Reihen, je nachdem ihre Differenz durch den Modul l theilbar ist, oder nicht. Wählt man aus jeder dieser Partialreihen nach Belieben ein Glied, so erhält man ein *vollständiges Restensystem* für den mod. l. Die *Anzahl* der Glieder eines solchen Restensystems ist immer gleich der Norm des Moduls $= N(l) = (a+b\varrho)(a+b\varrho^2) = a^2 - ab + b^2 = p$; wie sich leicht durch Betrachtungen zeigen läfst, denen ähnlich, welche *Gaufs* und *Dirichlet* bei den complexen Zahlen von der Form $a+b\sqrt{-1}$ angewandt haben.

Nehmen wir an, l sei eine von $1-\varrho$ und $1-\varrho^2$ verschiedene *complexe Primzahl* und

$$1. \quad R_1, \; R_2, \; \ldots\ldots \; R_{p-1}$$

ein vollständiges Restensystem für den Modul l, mit *Ausschlufs* des durch den Modul theilbaren Gliedes. Multiplicirt man sämmtliche Glieder dieses Restensystems mit einer nicht durch l theilbaren ganzen complexen Zahl A, so werden die Vielfachen

$$AR_1, \; AR_2, \; \ldots\ldots \; AR_{p-1}$$

wieder ein Restensystem von derselben Art wie das Restensystem (1.) bilden, und jedes dieser Vielfachen wird in (1.) sein entsprechendes Glied finden, welches ihm congruent ist. Man erhält daher, multiplicando,

$$A^{p-1} R_1 R_2 \ldots\ldots R_{p-1} \equiv R_1 R_2 \ldots\ldots R_{p-1} \pmod{l};$$

folglich, da das Product

$$R_1 R_2 \ldots\ldots R_{p-1}$$

nicht durch l theilbar ist,

$$2. \quad A^{p-1} \equiv 1 \pmod{l}.$$

Die Function $A^{p-1}-1$, welche also für jeden nicht durch l theilbaren Werth von A durch l theilbar ist, zerlegt sich in das Product von drei Ausdrücken

$$3. \quad (A^{\frac{1}{3}(p-1)}-1)(A^{\frac{1}{3}(p-1)}-\varrho)(A^{\frac{1}{3}(p-1)}-\varrho^2).$$

Von diesen drei Ausdrücken können nie zwei zugleich für denselben Werth von A durch l theilbar sein, weil sonst auch die Differenzen $1-\varrho$, $1-\varrho^2$ oder $\varrho-\varrho^2$ durch l theilbar sein müfsten, was nicht sein kann, da l von $1-\varrho$ und $1-\varrho^2$ verschieden ist. Auch kann keiner dieser drei Ausdrücke für mehr als $\frac{1}{3}(p-1)$ incongruente Werthe von A durch l theilbar werden. Setzt man also in das Product (3.) nach und nach statt A alle Glieder des Restensystems (1.), so wird jeder der drei Factoren *genau* für $\frac{1}{3}(p-1)$ Werthe von A durch l theilbar werden. Auf diese Weise theilen sich alle Glieder R des Restensystems (1.) in *drei* getrennte Classen. Für die Glieder der ersten Classe wird $R^{\frac{1}{3}(p-1)} \equiv 1 \pmod{l}$; für die der zweiten $R^{\frac{1}{3}(p-1)} \equiv \varrho \pmod{l}$, und für die Glieder der dritten Classe $R^{\frac{1}{3}(p-1)} \equiv \varrho^2 \pmod{l}$; und jede Classe enthält genau $\frac{1}{3}(p-1)$ Glieder. Dieselbe Classification dehnt sich über alle möglichen ganzen complexen Zahlen aus, in der Art, dafs je zwei ganze complexe Zahlen in dieselbe oder in verschiedene Classen gehören, je nachdem sie nach dem Modul l congruent sind, oder nicht.

Wir bezeichnen durch das Symbol

$$\left[\frac{A}{l}\right]$$

resp. eine der drei complexen Einheiten

$$1, \quad \varrho \quad \text{oder} \quad \varrho^2,$$

je nachdem man für die complexe Zahl A

$$A^{\frac{1}{3}(p-1)} \equiv 1 \quad \text{oder} \quad \equiv \varrho \quad \text{oder} \quad \equiv \varrho^2 \pmod{l}$$

hat, während l, wie immer, eine complexe Primzahl und p ihre Norm bezeichnet.

Man hat dann in allen Fällen

$$4. \qquad A^{\frac{1}{3}(p-1)} \equiv \left[\frac{A}{l}\right] \pmod{l}.$$

Der *cubische Character* der Zahl A in Beziehung auf den Modul ist derjenige Exponent k von ϱ, für welchen

$$A^{\frac{1}{3}(p-1)} \equiv \varrho^k \pmod{l} \text{ ist.}$$

Cubische Charactere, welche sich durch Vielfache der Zahl 3 von einander unterscheiden, sind demnach als aequivalent zu betrachten. Die Zahl A erhält den cubischen Character 0, 1 oder 2 in Beziehung auf den Modul l, je nachdem sie in die erste, zweite oder dritte der oben bezeichneten Classen gehört, oder, was dasselbe ist, je nachdem

$$\left[\frac{A}{l}\right] = 1 \quad \text{oder} \quad = \varrho \quad \text{oder} \quad = \varrho^2 \text{ ist.}$$

In Bezug auf die eben eingeführte Bezeichnung ergeben sich unmittelbar die folgenden einfachen Sätze.

„Wenn $A \equiv A \pmod{l}$, so hat man

$$5. \qquad \left[\frac{A}{l}\right] = \left[\frac{A'}{l}\right]."$$

Denn aus der Annahme $A \equiv A'$ folgt sogleich $A^{\frac{1}{3}(p-1)} \equiv A'^{\frac{1}{3}(p-1)}$.

„Alle Werthe von A, für welche $\left[\frac{A}{l}\right]$ denselben Werth erhält, sind in $\frac{1}{3}(p-1)$ linearen Formen enthalten."

„Wenn $\left[\frac{A}{l}\right] = 1$ ist, so ist A *cubischer Rest* für den Modul l; und ist umgekehrt A cubischer Rest zu l, so hat man nothwendig $\left[\frac{A}{l}\right] = 1$."

Die zweite Behauptung ist am leichtesten zu beweisen; denn wenn A cubischer Rest zu l ist, so hat man eine Congruenz von der Form

$$A \equiv z^3 \pmod{l},$$

wo z eine ganze complexe Zahl ist. Hieraus folgt, wenn man beide Theile zur Potenz $\frac{1}{3}(p-1)$ erhebt,

$$A^{\frac{1}{3}(p-1)} \equiv z^{p-1} \equiv 1 \pmod{l},$$

also $\left[\frac{A}{l}\right] = 1$. Der umgekehrte Satz ergiebt sich, wenn man bedenkt, dafs

die Anzahl der Glieder in dem Restensysteme (1.), welche cubische Reste für den mod. l sein können, genau $\frac{1}{3}(p-1)$ beträgt. In der That: da je drei associirte complexe Zahlen, wie

$$R, \quad \varrho R, \quad \varrho^2 R,$$

incongruent sind, aber zum Cubus erhoben dasselbe Resultat geben, und da umgekehrt aus $R^3 \equiv A^3$ immer nothwendig folgt, entweder $A \equiv R$ oder $A \equiv \varrho R$ oder $A \equiv \varrho^2 R$, so sieht man, dafs die Anzahl der nicht congruenten cubischen Reste sich genau auf den dritten Theil der überhaupt incongruenten (und nicht durch den Modul theilbaren) complexen Zahlen reducirt. Nun ist bereits bewiesen worden, dafs für alle cubischen Reste die Gleichung $\left[\frac{R}{l}\right] = 1$ Statt findet: wäre daher auch noch für einen nicht cubischen Rest diese Gleichung erfüllt, so würde es mehr als $\frac{1}{3}(p-1)$ Wurzeln der Congruenz

$$R^{\frac{1}{3}(p-1)} \equiv 1 \text{ (mod. } l)$$

geben; was nicht möglich ist.

„Die Congruenz und die Gleichung

$$6. \quad x^3 \equiv A \text{ (mod. } l), \quad \left[\frac{A}{l}\right] = 1$$

bedingen sich also gegenseitig."

„Der cubische Character eines Products ist (abgesehen von Vielfachen der Zahl 3) gleich der Summe der cubischen Charactere der einzelnen Factoren."

In der That, aus

$$(ABC\ldots.)^{\frac{1}{3}(p-1)} = A^{\frac{1}{3}(p-1)}.B^{\frac{1}{3}(p-1)}.C^{\frac{1}{3}(p-1)}\ldots. \text{ und}$$

$$(ABC\ldots.)^{\frac{1}{3}(p-1)} \equiv \left[\frac{ABC\ldots.}{l}\right], \quad A^{\frac{1}{3}(p-1)} \equiv \left[\frac{A}{l}\right] \text{ etc. (mod. } l)$$

folgt sogleich

$$7. \quad \left[\frac{ABC\ldots.}{l}\right] = \left[\frac{A}{l}\right]\left[\frac{B}{l}\right]\left[\frac{C}{l}\right]\ldots.;$$

worin der Beweis des Satzes liegt.

Kennt man also erst die cubischen Charactere aller complexen *Primzahlen*, so kann man den cubischen Character jeder beliebigen ganzen complexen Zahl leicht finden.

Einige specielle Fälle, welche bei der Operation mit diesen symbolischen Ausdrücken häufig vorkommen, sind die folgenden:

$$\left[\frac{A^2}{l}\right] = \left[\frac{A}{l}\right]^2 = \frac{1}{\left[\frac{A}{l}\right]},$$

$$\left[\frac{A^{3m+n}}{l}\right] = \left[\frac{A^n}{l}\right] = \left[\frac{A}{l}\right]^n.$$

„Wenn der Modul l *reell*, also einer reellen Primzahl von der Form $3n+2$ gleich ist, und A ebenfalls *reell* ist, so ist immer $\left[\frac{A}{l}\right]=1$."

In diesem Falle hat man $N(l)=l^2$; von der andern Seite läfst sich die Potenz $A^{\frac{1}{3}(l^2-1)}$ so schreiben: $(A^{\frac{1}{3}(l+1)})^{l-1}$; also hat man, weil A reell und $\frac{1}{3}(l+1)$ eine ganze Zahl ist, nach dem *Fermat*schen Satze, $A^{\frac{1}{3}(l^2-1)}\equiv 1$ (mod. l).

„Wenn $a+b\varrho$ irgend eine ganze complexe Zahl und $\alpha+\beta\varrho$ eine nicht in $a+b\varrho$ aufgehende complexe Primzahl ist, so findet die Relation

$$8.\quad \left[\frac{a+b\varrho}{\alpha+\beta\varrho}\right]=\left[\frac{a+b\varrho^2}{\alpha+\beta\varrho^2}\right]^2=\left[\frac{(a+b\varrho^2)^2}{\alpha+\beta\varrho^2}\right]$$

Statt." Denn bezeichnet man durch p die gemeinschaftliche Norm der beiden complexen Primzahlen $\alpha+\beta\varrho$ und $\alpha+\beta\varrho^2$, so ergiebt sich

$$\left[\frac{a+b\varrho}{\alpha+\beta\varrho}\right]=\varrho^k\equiv(a+b\varrho)^{\frac{1}{3}(p-1)}\ (\text{mod.}\ \alpha+\beta\varrho)$$
$$=(a+b\varrho)^{\frac{1}{3}(p-1)}+(m+n\varrho)(\alpha+\beta\varrho),$$

folglich auch, wenn man ϱ mit ϱ^2 vertauscht,

$$\varrho^{2k}=(a+b\varrho^2)^{\frac{1}{3}(p-1)}+(m+n\varrho^2)(\alpha+\beta\varrho^2),\ \text{also}$$
$$\varrho^{2k}\equiv(a+b\varrho^2)^{\frac{1}{3}(p-1)}\ (\text{mod.}\ \alpha+\beta\varrho^2),$$
$$\varrho^{k}\equiv(a+b\varrho^2)^{\frac{2}{3}(p-1)}\ (\text{mod.}\ \alpha+\beta\varrho^2),$$

folglich u. s. w.

Einen Satz, welcher zwar für das Folgende nicht nothwendig ist, wollen wir seiner Merkwürdigkeit wegen nicht übergehen.

„Bringt man die Glieder des Restensystems (1.) in folgende Ordnung:

I.	II.	III.
R_1	ϱR_1	$\varrho^2 R_1$
R_2	ϱR_2	$\varrho^2 R_2$
R_3	ϱR_3	$\varrho^2 R_3$
⋮	⋮	⋮
$R_{\frac{1}{3}(p-1)}$	$\varrho R_{\frac{1}{3}(p-1)}$	$\varrho^2 R_{\frac{1}{3}(p-1)}$,

und bezeichnet durch α, β, γ resp. die Anzahlen der Glieder der Reihe

$$AR_1,\ AR_2,\ AR_3,\ \ldots\ AR_{\frac{1}{3}(p-1)},$$

welche ihre congruenten Zahlen in (I.), (II), (III.) haben, so ist

$$10.\quad \left[\frac{A}{l}\right]=\varrho^{\beta+2\gamma}."$$

Um sich von der Möglichkeit einer solchen Anordnung zu überzeugen, nehme man irgend ein Glied R_1 aus (1.) und bilde die associirten ϱR_1, $\varrho^2 R_1$. Diese werden offenbar unter einander und zu R_1 incongruent sein, also beide ihr entsprechendes, von R_1 verschiedenes Glied in (1.) finden. Nachdem man diese drei Glieder aus (1.) gestrichen hat, nehme man irgend ein Glied von den übrig bleibenden R_2 und bilde die Reste von ϱR_2, $\varrho^2 R_2$; die so erhaltenen drei neuen Glieder werden unter einander und von den vorigen drei verschieden sein. Nachdem man sie gestrichen hat, wähle man unter den übrig bleibenden R_3, und bilde die Reste von ϱR_3 und $\varrho^2 R_3$; die drei neuen Glieder werden unter einander und von allen vorigen verschieden sein. Fährt man auf diese Weise fort, so wird man endlich das Restensystem (1.) vollständig erschöpft haben.

Die Vielfachen AR_1, AR_2 etc. $AR^{\frac{1}{3}(p-1)}$ sind alle nach dem mod. l incongruent; ich behaupte aber auch, dafs nie zwei derselben ihren Rest in derselben Horizontalreihe des Restensystems (9.) haben können; denn wäre dies der Fall, so müfste eine Congruenz von der Form $AR_\mu \equiv \varrho^k AR_\nu$ Statt finden, während k nicht durch 3 theilbar ist und μ und ν verschieden sind und in der Reihe von 1 bis $\frac{1}{3}(p-1)$ liegen. Hieraus würde aber folgen, da A nicht durch l theilbar ist: $R_\mu \equiv \varrho^k R_\nu$ (mod. l); was der Natur des Restensystems (9.) widerstreitet. Jene Vielfachen von A theilen sich demnach in drei Gruppen, je nachdem ihre Reste von der Form

$$R_\lambda, \quad R_{\lambda'}, \quad R_{\lambda''}, \quad \ldots,$$

oder von der Form

$$\varrho R_\mu, \quad \varrho R_{\mu'}, \quad \varrho R_{\mu''}, \quad \ldots,$$

oder endlich von der Form

$$\varrho^2 R_\nu, \quad \varrho^2 R_{\nu'}, \quad \varrho^2 R_{\nu''}, \quad \ldots$$

sind; so jedoch, dafs alle die Zahlen

$$R_\lambda, R_{\lambda'}, R_{\lambda''}, \ldots, \quad R_\mu, R_{\mu'}, R_{\mu''}, \ldots, \quad R_\nu, R_{\nu'}, R_{\nu''}, \ldots$$

zusammengenommen wieder die vollständige Reihe

$$R_1, \quad R_2, \quad R_3, \quad \ldots \quad R_{\frac{1}{3}(p-1)}$$

bilden. Hieraus folgt, da die Anzahlen der in diesen Gruppen enthaltenen Glieder resp. durch α, β, γ bezeichnet worden sind:

$$A^{\frac{1}{3}(p-1)} R_1 R_2 R_3 \ldots R_{\frac{1}{3}(p-1)} \equiv \varrho^{\beta+2\gamma} R_1 R_2 R_3 \ldots R_{\frac{1}{3}(p-1)},$$

folglich, da das Product

$$R_1 R_2 R_3 \ldots R_{\frac{1}{3}(p-1)}$$

nicht durch den Modul l theilbar ist,

$$A^{\frac{1}{3}(p-1)} \equiv \varrho^{\beta+2\gamma} \pmod{l};$$

was zu beweisen war.

§. 3.

Wir beziehen uns jetzt auf einige Formeln, die in einer früheren Abhandlung („*Beiträge zur Kreistheilung*") bewiesen wurden. Wenn p eine reelle Primzahl ist, ω und r primitive $p-1$te und $p$te Wurzeln der Einheit vorstellen, Ind. k für eine zur Primzahl p gehörige primitive Congruenzwurzel g diejenige Zahl μ bezeichnet, welche der Congruenz $g^{\mu} \equiv k \pmod{p}$ genügt, und man setzt, ganz wie in der citirten Abhandlung,

$$1. \quad \varphi(\alpha, \beta) = \sum_{k=1}^{k=p-1} \omega^{\alpha \operatorname{Ind.} k}\, r^{\beta k} \text{ und}$$

$$2. \quad S[\alpha, \beta] = \sum_{\sigma=1}^{\sigma=p-2} \omega^{\alpha \operatorname{Ind.} \sigma - (\alpha+\beta) \operatorname{Ind.} (\sigma+1)},$$

so wurde gefunden:

$$3. \quad \varphi(\alpha, \beta) = \omega^{-\alpha \operatorname{Ind.} \beta}\, \varphi(\alpha, 1) \text{ und}$$

$$4. \quad \frac{\varphi(\alpha, 1)\, \varphi(\beta, 1)}{\varphi(\alpha+\beta, 1)} = S[\alpha, \beta],$$

wenn keine der drei Zahlen α, β und $\alpha+\beta$ durch $p-1$ theilbar ist; ferner

$$5. \quad S[\alpha, \beta]\, S[-\alpha, -\beta] = p;$$

und endlich, wenn α ein Theiler von $p-1$ und $p-1 = m\alpha$ ist,

$$6. \quad \varphi(\alpha, 1)^m = (-1)^{\alpha} p\, S[\alpha, \alpha]\, S[\alpha, 2\alpha] \ldots . S[\alpha, (m-2)\alpha].$$

Die Beweise, welche von diesen Formeln gegeben wurden, waren höchst einfach und setzten nichts aus der Kreistheilung selbst als bekannt voraus. Sie gründeten sich nur auf das Princip, dafs für jede, nicht durch p theilbare Zahl m die Reste der Vielfachen

$$m, \quad 2m, \quad 3m, \quad \ldots . \quad (p-1)m$$

die Reihe

$$1, \quad 2, \quad 3, \quad \ldots . \quad p-1$$

reproduciren, und darauf, dafs man in einer Doppelreihe die Ordnung der Summationen umkehren darf.

Wendet man diese Formeln auf den speciellen Fall an, in welchem p eine Primzahl von der Form $3n+1$, und $\alpha = \frac{1}{3}(p-1)$ ist, so erhält man, weil jetzt α gerade ist und die Potenz $\omega^{\frac{1}{3}(p-1)}$ durch die imaginäre Cubikwurzel ϱ ersetzt werden kann, aus der Formel (6.):

$$7. \quad \left(\sum_{k=1}^{k=p-1} \varrho^{\operatorname{Ind.} k}\, r^k\right)^3 = p \sum_{\sigma=1}^{\sigma=p-2} \varrho^{\operatorname{Ind.} \sigma + \operatorname{Ind.} (\sigma+1)} = p(\mu + \nu\varrho),$$

und ebenso, wenn man ϱ^2 statt ϱ setzt,

$$8.\quad \left(\sum_{k=1}^{k=p-1} \varrho^{2\,\mathrm{Ind.}\,k}\, r^k\right)^3 = p\sum_{\sigma=1}^{\sigma=p-2} \varrho^{2(\mathrm{Ind.}\,\sigma+\mathrm{Ind.}(\sigma+1))} = p(\mu+\nu\varrho^2);$$

wo μ und ν reelle Zahlen sind.

Aus (5.) ergiebt sich ferner für diesen Fall

$$9.\quad (\mu+\nu\varrho)(\mu+\nu\varrho^2) = p$$

und aus (3.)

$$10.\quad \sum_{k=1}^{k=p-1} \varrho^{\mathrm{Ind.}\,k}\, r^{\beta k} = \varrho^{2\,\mathrm{Ind.}\,\beta} \sum_{k=1}^{k=p-2} \varrho^{\mathrm{Ind.}\,k}\, r^k.$$

Ich behaupte jetzt, dafs die ganzen Zahlen μ und ν, wie sie sich aus

$$\sum_{\sigma=1}^{\sigma=p-2} \varrho^{\mathrm{Ind.}\,\sigma+\mathrm{Ind.}(\sigma+1)} = \mu+\nu\varrho$$

berechnen lassen, immer den beiden Congruenzen

$$11.\quad \mu \equiv 2 \pmod{3},\quad \nu \equiv 0 \pmod{3}.$$

genügen. Entwickelt man in der That nach dem polynomischen Lehrsatze den Cubus der Reihe

$$\sum \varrho^{\mathrm{Ind.}\,k}\, r^k,$$

welcher $= p(\mu+\nu\varrho)$ ist, und sondert von der ganzen Entwicklung die Cuben der einzelnen Glieder der Reihe ab, nämlich

$$r^3,\quad r^6,\quad r^9,\quad \ldots\ldots\quad r^{3(p-1)},$$

so werden die Coëfficienten aller übrig bleibenden Glieder durch 3 theilbar sein, und die Summe dieser übrig bleibenden Glieder wird die Form $3W$ haben, wo W eine ganze Function der $p$ten Wurzeln der Einheit mit ganzen complexen Coëfficienten ist. Da nun

$$r^3+r^6+r^9+\ldots\ldots+r^{3(p-1)} = -1$$

ist, so hat man

$$3W = p\mu+1+p\nu\varrho,$$

folglich nach dem *vierten Hülfssatze* (§. 1.),

$$p\mu+1+p\nu\varrho \equiv 0 \pmod{3}.\quad \text{Aber es ist}\quad p \equiv 1 \pmod{3},$$

also ist nothwendig $\mu+1$, und ν durch 3 theilbar.

Nennen wir jede complexe Primzahl, welche $\equiv 2 \pmod{3}$ ist, *primäre* complexe Primzahl, so sind nach dieser Definition und nach dem eben Bewiesenen $\mu+\nu\varrho$ und $\mu+\nu\varrho^2$ primäre complexe Primzahlen.

Jede reelle Primzahl p von der Form $3n+1$ kann offenbar *nur auf eine Weise* in das Product zweier primären complexen Primzahlen zerlegt werden, wenn man die beiden, durch blofse Permutation aus einander hervor-

gehenden Zerlegungen $p=(a+b\varrho)(a+b\varrho^2)=p_1p_2$ und $p=p_2p_1$ als identisch betrachtet.

Es sei also *a priori* p in das Product der beiden primären complexen Primzahlen p_1p_2 zerlegt. Dann mufs nothwendig $\mu+\nu\varrho$ wegen (9.) mit einer der beiden Primzahlen p_1 oder p_2 zusammenfallen; aber es hängt lediglich von der Wahl der primitiven Congruenzwurzel g ab, ob $\mu+\nu\varrho=p_1$ oder $\mu+\nu\varrho=p_2$ ist.

Um zu bestimmten Resultaten zu gelangen, die von der Wahl der primitiven Wurzel unabhängig sind, wollen wir annehmen, es sei g so gewählt, dafs sie der Congruenz

$$12.\qquad g^{\frac{1}{3}(p-1)} \equiv \varrho \pmod{p_1}$$

genügt. Diese Bedingung ist immer zulässig und sie wird genau von der Hälfte aller primitiven Congruenzwurzeln erfüllt. In der That: zunächst kann nie $g^{\frac{1}{3}(p-1)}\equiv 1 \pmod{p_1}$ sein, weil sonst $g^{\frac{1}{3}(p-1)}-1$ durch p_1, also, da der Ausdruck reell ist, auch durch p_2, folglich durch p theilbar sein würde; was dem Begriff der primitiven Wurzel widerstreitet. Es kann also nur entweder

$$(A.)\qquad g^{\frac{1}{3}(p-1)} \equiv \varrho \pmod{p_1},\ \text{oder}$$
$$(B.)\qquad g^{\frac{1}{3}(p-1)} \equiv \varrho^2 \pmod{p_1}$$

sein. Da die Congruenzen (*A.*), (*B.*), wenn man beide Seiten zur Potenz $p-2$ erhebt, resp. Congruenzen von der Form (*B.*) oder (*A.*) hervorbringen, wo nur g^{p-2} statt g steht, und da g^{p-2} ebenfalls eine primitive Congruenzwurzel ist, wenn g es ist, so folgt, dafs die Hälfte aller Congruenzwurzeln g der Congruenz (*A.*) und die andere Hälfte der Congruenz (*B.*) genügt.

Unter der Voraussetzung (12.) hat man für jeden Werth k, von 1 bis $p-1$,

$$g^{\frac{1}{3}(p-1)\,\text{Ind.}\,k} \equiv \varrho^{\text{Ind.}\,k} \pmod{p_1},\ \text{also}$$
$$13.\qquad k^{\frac{1}{3}(p-1)} \equiv \varrho^{\text{Ind.}\,k} \pmod{p_1},$$
$$14.\qquad \varrho^{\text{Ind.}\,k} = \left[\frac{k}{p_1}\right].$$

Ich behaupte jetzt, dafs nach der in (12.) gemachten Annahme nothwendig

$$\sum_{\sigma=1}^{\sigma=p-2} \varrho^{\text{Ind.}\,\sigma+\text{Ind.}\,(\sigma+1)} = p_1$$

sein mufs und dafs dieselbe Summe *nicht* $=p_2$ sein kann.

Da man nur die Wahl zwischen den beiden Werthen p_1 und p_2 hat, so handelt es sich darum, zu zeigen, dafs der Werth p_2 unstatthaft ist. Nach

der Gleichung (13.) erhält man

$$15. \quad \sum_{\sigma=1}^{\sigma=p-2} \varrho^{\text{Ind.}\sigma+\text{Ind.}(\sigma+1)} \equiv \sum_{\sigma=1}^{\sigma=p-2} \sigma^{\frac{1}{3}(p-1)}(\sigma+1)^{\frac{1}{3}(p-1)} \pmod{p_1}.$$

Die Reihe auf der rechten Seite ist genau von der Form derjenigen, welche wir in dem 6ten Hülfssatze des ersten Paragraphen betrachtet haben. Es ist hier $m=\frac{1}{3}(p-1)$, $n=\frac{1}{3}(p-1)$ und $m+n=\frac{2}{3}(p-1)<p-1$; also ist nach jenem Satze der Werth der Reihe auf der rechten Seite der Congruenz (15.) durch p und mithin um so mehr durch p_1 theilbar. Hieraus folgt, wegen (15.),

$$\sum_{\sigma=1}^{\sigma=p-2} \varrho^{\text{Ind.}\sigma+\text{Ind.}(\sigma+1)} \equiv 0 \pmod{p_1}.$$

Wäre nun, gegen die Behauptung, diese Reihe $=p_2$, so würde p_2 durch p_1 theilbar sein; was unmöglich ist, da p_2 eine complexe Primzahl und nicht zu p_1 associirt ist; also ist die Reihe nothwendig $=p_1$.

Nachdem wir uns so von der Richtigkeit obiger Behauptung überzeugt haben, wollen wir in den Formeln (7.) und (10.) statt $\varrho^{\text{Ind.}k}$ die symbolische Bezeichnung aus der Gleichung (14.) einführen. Geschieht dies, so kommt

$$16. \quad \left(\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right] r^k\right)^3 = p\,p_1 \text{ und}$$

$$17. \quad \Sigma\left[\frac{k}{p_1}\right] r^{gk} = \left[\frac{g^2}{p_1}\right]\Sigma\left[\frac{k}{p_1}\right] r^k \quad \left\{\begin{matrix} k=1 \text{ bis} \\ k=p-1 \end{matrix}\right\};$$

und diese beiden Resultate enthalten nichts, was an die Wahl einer primitiven Wurzel erinnern könnte.

Nach diesen Vorbereitungen läfst sich nun zu dem Hauptgegenstande dieser Abhandlung übergehen.

§. 4.

Beweis des cubischen Reciprocitätssatzes.

Fundamental-Theorem.

„Wenn l und l' irgend zwei primäre complexe Primzahlen mit „verschiedener Norm sind (so dafs $l\equiv l'\equiv 2 \pmod{3}$), *so ist immer der „cubische Character der ersten in Bezug auf die zweite gleich dem cu- „bischen Character der zweiten in Bezug auf die erste; oder in Zeichen: „es ist immer*

$$\left[\frac{l}{l'}\right] = \left[\frac{l'}{l}\right].$$

Beweis.

Alle primären complexen Primzahlen zerfallen in zwei grofse Classen. Die Primzahlen von der ersten Classe sind *eingliedrig* und fallen mit den reellen Primzahlen von der Form $3n+2$ zusammen; ihre Norm ist dem Quadrate der Primzahl gleich. Die Primzahlen zweiter Classe sind *zweigliedrig* und entstehen aus der Zerlegung der reellen Primzahlen von der Form $3n+1$ in ihre beiden primären complexen Primfactoren; die reelle Primzahl von der Form $3n+1$ erscheint dann als die gemeinschaftliche Norm ihrer beiden complexen Primfactoren *).

Wenn es sich daher, wie hier, um den cubischen Character zweier primären complexen Primzahlen in Bezug auf einander handelt, so sind drei Fälle zu unterscheiden.

I. Wenn beide Primzahlen eingliedrig sind.

II. Wenn die eine Primzahl eingliedrig, die andere zweigliedrig ist; und endlich:

III. Wenn beide Primzahlen zweigliedrig sind.

Beweis des ersten Falles.

Wenn p und q zwei reelle Primzahlen $3n+2$ sind, so hat man nach §. 2.

$$\left[\frac{p}{q}\right] = 1 \quad \text{und} \quad \left[\frac{q}{p}\right] = 1,$$

also gewifs

$$\left[\frac{p}{q}\right] = \left[\frac{q}{p}\right]. \quad \text{(Erster Fall.)}$$

Beweis des zweiten Falles.

Es sei p eine reelle Primzahl $3n+1$, q eine reelle Primzahl $3n+2$; p_1 und p_2 seien die beiden primären complexen Primzahlen, in welche p zerlegt werden kann, so dafs $p = p_1 p_2$ ist.

Wenn man

$$\left[\frac{k}{p_1}\right] r^k = T, \qquad \Sigma \left[\frac{k}{p_1}\right] r^{\beta k} = T_\beta$$

setzt, wo die Summationen sich von $k=1$ bis $k=p-1$ erstrecken, und

*) So hat man z. B. $7 = (2+3\varrho)(2+3\varrho^2)$, $13 = (-1+3\varrho)(-1+3\varrho^2)$, $19 = (5+3\varrho)(5+3\varrho^2)$ etc., also sind $\begin{matrix} 2+3\varrho, & -1+3\varrho, & 5+3\varrho \\ 2+3\varrho^2, & -1+3\varrho^2, & 5+3\varrho^2 \end{matrix}$ etc. primäre complexe Primzahlen 2ter Classe, während 2, 5, 11, 17 etc. primäre complexe Primzahlen erster Classe sind.

hier $\beta = q^2$ nimmt, so ist nach (16.) und (17.) des vorigen Paragraphen:

$$(A.)\qquad T^3 = pp_1,$$

$$(B.)\qquad T_{q^2} = \left[\frac{q}{p_1}\right] T.$$

Erhebt man die Formel (A.) zur Potenz $\frac{1}{3}(q^2-1)$, so kommt

$$(C.)\qquad T^{q^2-1} = (pp_1)^{\frac{1}{3}(q^2-1)}.$$

Multiplicirt man ferner die (C.) mit T^3, die (B.) mit T^2, und subtrahirt das zweite Resultat vom ersten, so erhält man

$$(D.)\qquad T^2(T^{q^2} - T_{q^2}) = T^3.\left\{(pp_1)^{\frac{1}{3}(q^2-1)} - \left[\frac{q}{p_1}\right]\right\},$$

und wenn man hier nach (A.) T^3 durch pp_1 ersetzt,

$$(E.)\qquad T^2(T^{q^2} - T_{q^2}) = pp_1\left\{(pp_1)^{\frac{1}{3}(q^2-1)} - \left[\frac{q}{p_1}\right]\right\}.$$

Die Potenz T^{q^2}, nach dem polynomischen Satze entwickelt, giebt lauter durch q theilbare Glieder, mit Ausschlufs derjenigen Glieder, welche die q^2ten Potenzen der einzelnen Glieder von T selbst repräsentiren, nämlich der Glieder von der Form

$$\left(\left[\frac{k}{p_1}\right] r^k\right)^{q^2} = \left[\frac{k}{p_1}\right]^{q^2} r^{q^2 k} = \left[\frac{k}{p_1}\right] r^{q^2 k}.$$

Diese Glieder sind aber gerade diejenigen, welche die Reihe

$$T_{q^2}$$

zusammensetzen; also sind alle Glieder der Differenz

$$T^{q^2} - T_{q^2},$$

folglich auch alle Glieder der entwickelten linken Seite in (E.) durch q theilbar. Wir schliefsen demnach aus (E.) nach dem vierten Hülfssatze (§. 1.) die Congruenz

$$pp_1.\left\{(pp_1)^{\frac{1}{3}(q^2-1)} - \left[\frac{q}{p_1}\right]\right\} \equiv 0 \pmod{q},$$

folglich, da der Factor pp_1 nicht durch q theilbar ist,

$$(F.)\qquad (pp_1)^{\frac{1}{3}(q^2-1)} \equiv \left[\frac{q}{p_1}\right] \pmod{q}.$$

Diese Congruenz giebt, wenn wir ihren Sinn auf die symbolische Bezeichnung übertragen,

$$\left[\frac{pp_1}{q}\right] = \left[\frac{q}{p_1}\right];$$

folglich, wegen

$$\left[\frac{pp_1}{q}\right] = \left[\frac{p}{q}\right]\left[\frac{p_1}{q}\right] \text{ und } \left[\frac{p}{q}\right] = 1,$$

$$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right].\ \text{(Zweiter Fall.)}$$

Beweis des dritten Falles.

Es seien p und q zwei verschiedene reelle Primzahlen von der Form $3n+1$; beide seien in ihre primären complexen Primzahlen zerlegt, nämlich

$$p = p_1 p_2, \quad q = q_1 q_2,$$

so dafs p_1, p_2, q_1, q_2 zweigliedrige primäre complexe Primzahlen sind.

Setzt man wieder, wie oben,

$$\Sigma\left[\frac{k}{p_1}\right] r^k = T, \quad \Sigma\left[\frac{k}{p_1}\right] r^{\beta k} = T_\beta,$$

wo die Summationen sich ebenfalls von $k=1$ bis $k=p-1$ erstrecken, nimmt aber diesmal $\beta=q$, so ist nach (16.) und (17.) (§. 3.)

$$(A.) \quad T^3 = pp_1 \text{ und}$$

$$(B.) \quad T_q = \left[\frac{q^2}{p_1}\right] T.$$

Die Gleichung $(A.)$, zur Potenz $\frac{1}{3}(q-1)$ erhoben, giebt

$$(C.) \quad T^{q-1} = (pp_1)^{\frac{1}{3}(q-1)}.$$

Multiplicirt man $(C.)$ mit T^3, $(B.)$ mit T^2, und subtrahirt, so kommt

$$(D.) \quad T^2(T^q - T_q) = T^3\left\{(pp_1)^{\frac{1}{3}(q-1)} - \left[\frac{q^2}{p_1}\right]\right\};$$

folglich, wenn man rechts den Werth pp_1 für T^3 setzt,

$$(E.) \quad T^2(T^q - T_q) = pp_1\left\{(pp_1)^{\frac{1}{3}(q-1)} - \left[\frac{q^2}{p_1}\right]\right\}.$$

Entwickelt man den Ausdruck links nach dem polynomischen Satze, so überzeugt man sich leicht, dafs die Coëfficienten aller seiner Glieder durch q theilbar werden. Wir schliefsen hieraus nach dem 4ten Hülfssatze (§. 1.), dafs die Congruenz

$$pp_1\left\{(pp_1)^{\frac{1}{3}(q-1)} - \left[\frac{q^2}{p_1}\right]\right\} \equiv 0 \pmod{q}$$

Statt findet, oder, da pp_1 zum Modul q relative Primzahl ist,

$$(F.) \quad (pp_1)^{\frac{1}{3}(q-1)} \equiv \left[\frac{q^2}{p_1}\right] \pmod{q}.$$

Da demnach der Ausdruck $(pp_1)^{\frac{1}{3}(q-1)} - \left[\frac{q^2}{p_1}\right]$ durch q theilbar und $q=q_1q_2$ ist, so wird derselbe Ausdruck um so mehr noch einzeln durch q_1 und durch q_2 theilbar sein. Die Congruenz $(F.)$ zerlegt sich demnach in die beiden folgenden:

$$(G.) \quad (pp_1)^{\frac{1}{3}(q-1)} \equiv \left[\frac{q^2}{p_1}\right] \pmod{q_1},$$

$$(H.) \quad (pp_1)^{\frac{1}{3}(q-1)} \equiv \left[\frac{q^2}{p_1}\right] \pmod{q_2}.$$

Aus diesen beiden Congruenzen und denjenigen, welche aus ihnen hervorgehen, wenn man p_1 mit p_2 vertauscht, nämlich

$$(I.)\qquad (pp_2)^{\frac{1}{3}(q-1)} \equiv \left[\frac{q^2}{p_2}\right] \text{ (mod. } q_1) \text{ und}$$

$$(K.)\qquad (pp_2)^{\frac{1}{3}(q-1)} \equiv \left[\frac{q^2}{p_2}\right] \text{ (mod. } q_2),$$

ziehen wir die folgenden Gleichungen:

$$(\alpha.)\qquad \left[\frac{pp_1}{q_1}\right] = \left[\frac{pp_1}{q_2}\right] = \left[\frac{q^2}{p_1}\right] = \left[\frac{q}{p_2}\right],$$

$$(\beta.)\qquad \left[\frac{pp_2}{q_1}\right] = \left[\frac{pp_2}{q_2}\right] = \left[\frac{q^2}{p_2}\right] = \left[\frac{q}{p_1}\right].$$

Vertauschen wir jetzt die reellen Primzahlen p und q mit einander, was offenbar erlaubt ist, da p und q beide von der Form $3n+1$ sind, und da wir in der ganzen Untersuchung ebensowohl q wie p als die ursprüngliche Primzahl annehmen konnten, so müssen auch p_1 und q_1, so wie p_2 und q_2, ihrerseits mit einander verwechselt werden. Die Gleichungen (α.) und (β.) liefern auf diese Weise noch die folgenden beiden:

$$(\gamma.)\qquad \left[\frac{qq_1}{p_1}\right] = \left[\frac{qq_1}{p_2}\right] = \left[\frac{p^2}{q_1}\right] = \left[\frac{p}{q_2}\right],$$

$$(\delta.)\qquad \left[\frac{qq_2}{p_1}\right] = \left[\frac{qq_2}{p_2}\right] = \left[\frac{p^2}{q_2}\right] = \left[\frac{p}{q_1}\right].$$

Multiplicirt man die Gleichung (β.) mit $\left[\frac{q_1}{p_1}\right]$, so kommt

$$\left[\frac{pp_2}{q_1}\right]\left[\frac{q_1}{p_1}\right] = \left[\frac{q}{p_1}\right]\left[\frac{q_1}{p_1}\right] = \left[\frac{qq_1}{p_1}\right].$$

Aber nach (γ.) ist

$$\left[\frac{qq_1}{p_1}\right] = \left[\frac{p^2}{q_1}\right], \text{ also } \left[\frac{pp_2}{q_1}\right]\left[\frac{q_1}{p_1}\right] = \left[\frac{p^2}{q_1}\right] = \left[\frac{pp_2}{q_1}\right]\left[\frac{p_1}{q_1}\right],$$

folglich, wenn man auf beiden Seiten den gemeinschaftlichen Factor

$$\left[\frac{pp_2}{q_1}\right]$$

wegläfst,

$$\left[\frac{q_1}{p_1}\right] = \left[\frac{p_1}{q_1}\right].\quad \text{(Dritter Fall.)}$$

Das cubische Reciprocitätsgesetz, welches zwischen je zwei primären complexen Primzahlen $a+b\varrho$ Statt findet, ist also hierdurch für alle Fälle bewiesen.

Da -1, wegen $(-1)^3 = -1$, zu jedem Modul cubischer Rest ist, so hat man $\left[\frac{-1}{q}\right] = 1$ und $\left[\frac{-1}{p}\right] = 1$, folglich

$$\left[\frac{-1}{l'}\right] = \left[\frac{l}{l'}\right], \quad \left[\frac{-l'}{l}\right] = \left[\frac{l'}{l}\right];$$

und da das Zeichen des Moduls selbst offenbar ganz gleichgültig ist, so sieht man, dafs die oben beim Reciprocitätsgesetze gemachte Bedingung, dafs l und l' primär sein sollen, nicht mehr nöthig ist, sondern dafs nur

$$l \equiv \pm 1 \text{ (mod. 3)} \quad \text{und} \quad l' \equiv \pm 1 \text{ (mod. 3)}$$

erforderlich ist; so dafs also für je zwei complexe Primzahlen, bei denen der Coëfficient von ϱ durch 3 theilbar ist und deren Normen verschieden sind, die Gleichung

$$\left[\frac{l}{l'}\right] = \left[\frac{l'}{l}\right]$$

Statt findet.

Die Folgerungen, welche man aus diesem merkwürdigen Satze ziehen kann, sind sehr zahlreich. Es ergiebt sich unmittelbar aus demselben, dafs alle complexen Primtheiler der Ausdrücke von der Form

$$z^3 - l,$$

wo z eine bestimmte complexe ganze Zahl vorstellt, in gewissen linearen Formen enthalten, d. h. Glieder complexer arithmetischer Reihen sind, deren Anfangsglieder complexe ganze Zahlen sind und deren Differenz l ist.

So sind z. B. die Theiler des Ausdrucks

$$z^3 - (2 + 3\varrho)$$

in den beiden Formen

$$(2+3\varrho)(m+n\varrho)+1, \qquad (2+3\varrho)(m+n\varrho)-1$$

enthalten, wo m und n alle möglichen reellen ganzen Zahlen vorstellen.

Derselbe Satz läfst sich auch leicht auf zusammengesetzte Zahlen, d. h. allgemein auf Ausdrücke von der Form

$$z^3 - D$$

ausdehnen, wo D irgend eine gegebene ganze complexe Zahl vorstellt; ganz in derselben Weise, wie man es bei den quadratischen Resten in der reellen Theorie thut.

Die schöne Erweiterung, welche Herr Professor *Jacobi* dem *Legendre*-schen Zeichen gegeben hat, läfst sich auch bei den Ausdrücken $\left[\frac{A}{l}\right]$ anbringen, welche bisher nur eine Bedeutung erhalten hatten, wenn l eine Prim-

zahl war. Wenn

$$L = ll'l''\dots$$

ist, wo l, l', l'', ... gleiche oder ungleiche complexe Primzahlen vorstellen, so sei die Definition des verallgemeinerten Symbols

$$\left[\frac{A}{L}\right],$$

wo A und L relative Primzahlen zu einander sind, durch folgende Gleichung festgestellt:

$$\left[\frac{A}{L}\right] = \left[\frac{A}{l}\right]\left[\frac{A}{l'}\right]\left[\frac{A}{l''}\right]\dots.$$

Dann ist, wenn L und L' irgend zwei ganze complexe Zahlen sind, für welche die Coëfficienten von ϱ durch 3 theilbar und deren Normen relative Primzahlen zu einander sind, ganz wie bei Primzahlen:

$$\left[\frac{L}{L'}\right] = \left[\frac{L'}{L}\right].$$

Denn man kann immer

$$L = l_1 l_2 l_3 \dots l_m = \Pi l_\sigma \text{ und}$$
$$L' = l'_1 l'_2 l'_3 \dots l'_n = \Pi l'_\tau$$

setzen, wo l_1 etc., l'_1 etc. complexe Primzahlen und sämmtlich $\equiv \pm 1 \pmod{3}$ sind, und wo keine von den Normen der l mit irgend einer von den Normen der l' identisch ist. Man hat dann nach der Definition, zufolge eines in §. 2 bewiesenen Satzes und nach dem Fundamentaltheorem:

$$\left[\frac{L}{L'}\right] = \Pi^\tau \left[\frac{L}{l'_\tau}\right] = \Pi^\tau \Pi^\sigma \left[\frac{l_\sigma}{l'_\tau}\right] = \Pi^\tau \Pi^\sigma \left[\frac{l'_\tau}{l_\sigma}\right] = \Pi^\sigma \left[\frac{L'}{l_\sigma}\right] = \left[\frac{L'}{L}\right],$$

w. z. b. w.

Alle diese Sätze bilden die Grundlage zu einer der schönsten Theorieen der höheren Arithmetik, nämlich zu der Theorie der Theiler der Ausdrücke von der Form

$$x^3 + DD'y^3 + DD''z^3 - 3Dxyz,$$

wo D, D', D'' gegebene ganze complexe Zahlen sind und $D'D'' = D$ ist, und wo x, y, z unbestimmte ganze complexe Zahlen vorstellen; über welche Ausdrücke wir Untersuchungen angestellt haben, die wir später auseinanderzusetzen die Ehre haben werden.

Als ein wichtiges Complement zu dieser Theorie dient der Satz, dafs jede der linearen Formen, in welchen die Theiler begriffen sind, wirklich unendlich viele Primzahlen darstellt, oder überhaupt, dafs jede arithmetische Pro-

gression, deren erstes Glied und Differenz ganze complexe Zahlen $a+b\varrho$ ohne gemeinschaftlichen Theiler sind. unendlich viele complexe Primzahlen enthält. Der Beweis dieses Satzes kann mit Hülfe der schönen *Dirichletschen Principien* gegeben werden. Die Reihen, deren man sich bei der betreffenden Untersuchung zu bedienen hat, und welche auch bei der Bestimmung der Anzahl der quadratischen Formen in der Theorie dieser complexen Zahlen erscheinen, hangen mit der Theilung derjenigen elliptischen Functionen zusammen, welche aus unendlichen Doppelproducten bestehen, von der Form

$$\Pi\left(1-\frac{x}{\lambda+\lambda'\varrho}\right),$$

ebenso wie die entsprechenden Reihen in der Theorie der Zahlen $a+b\sqrt{-1}$ von der Theilung der Lemniscate abhangen. Die Theilung der eben erwähnten elliptischen Functionen läfst sich *algebraisch* ausführen, d. h. die Wurzeln der Gleichungen, von denen die Theilung abhangt, lassen sich durch Wurzelzeichen darstellen.

Berlin im März 1844.

22.

Über die Anzahl der quadratischen Formen in den verschiedenen complexen Theorieen.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

In einer früheren Note haben wir den Satz mitgetheilt, dafs in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen die Anzahl der quadratischen Formen für eine reelle Determinante $+D$ dem halben Producte der Formen-Anzahlen für die beiden Determinanten

$$+D \quad \text{und} \quad -3D$$

in der reellen Theorie gleich ist *).

Die Bestimmung der Formenzahl für diese complexen Zahlen hangt im *Allgemeinen*, d. h. für jede complexe Determinante, von der *Theilung* derjenigen elliptischen Functionen ab, welche Quotienten aus unendlichen Doppelproducten von der Form

$$\Pi\left(1-\frac{x}{\lambda+\lambda'\varrho}\right)$$

sind, wo ϱ eine imaginäre Cubikwurzel der Einheit ist und λ, λ' Indices bezeichnen. (Vergl. „Bemerkungen zu den elliptischen und Abelschen Transcendenten.")

Der obige Satz bezog sich auf *positive* Determinanten; die negativen Determinanten verhalten sich in dieser Theorie wesentlich anders: für diese Determinanten gilt folgender Satz:

„Für eine negative Determinante $-D$, wo D reell und positiv ist, ist die Anzahl der nicht-aequivalenten quadratischen Formen in der Theorie der Zahlen $a+b\varrho$ gleich dem Einfachen, oder gleich der Hälfte des Products aus den Formen-Anzahlen für die beiden Determinanten

$$-D \quad \text{und} \quad 3D$$

in der reellen Theorie, je nachdem die unbestimmte Gleichung

$$Dt^2-3u^2=1$$

in reellen ganzen Zahlen lösbar ist, oder nicht" **).

---

*) Die Fälle, in welchen D ein Quadrat ist, sind natürlich ausgenommen.

**) Ausgenommen werden die Fälle, wenn $3D$ ein Quadrat ist.

Zur Auffindung dieser merkwürdigen Resultate bedurfte ich besonders des folgenden Satzes über die Anzahl der zu derselben reellen Zahl als Norm gehörigen complexen Zahlen, als Hülfssatz. Unter *unähnlichen* complexen Zahlen sind solche zu verstehen, welche nicht durch Multiplication mit

$$\pm 1, \quad \pm \varrho \quad \text{oder} \quad \pm \varrho^2$$

auseinander entstehen können.

„Ist M eine beliebige, gegebene ganze positive Zahl und m das allgemeine Glied der Reihe ihrer sämmtlichen Theiler, 1 und M incl., so giebt die Reihe

$$\Sigma \left(\frac{-3}{m}\right),$$

wo $\left(\frac{-3}{m}\right) = 0,\ 1,$ oder -1 ist, je nachdem der Theiler m die Form $3n$, $3n+1$ oder $3n-1$ hat, die Anzahl der zu der Norm M gehörigen unähnlichen ganzen complexen Zahlen."

Dieser Satz kann unmittelbar aus den Elementen der complexen Zahlen $a+b\varrho$ abgeleitet werden.

Es bezeichne $N(a+b\varrho)$ die Norm der complexen Zahl $a+b\varrho$; ferner
μ alle möglichen unähnlichen ganzen complexen Zahlen;
λ alle unähnlichen complexen Primzahlen;
M alle positiven ganzen (reellen) Zahlen;
L alle reellen positiven Primzahlen, und unter ihnen
P die Primzahlen $3n+1$,
Q die Primzahlen $3n+2$.

Offenbar läfst sich jede complexe Zahl μ auf eine, und nur auf eine Art auf die Form

$$\mu = \lambda_1^{\alpha} \lambda_2^{\beta} \ldots.$$

bringen; es ist daher

$$\Sigma^{\mu} \frac{1}{N(\mu)^s} = \Sigma \frac{1}{N(\lambda_1^{\alpha} \lambda_2^{\beta} \ldots)^s} = \Pi^{\lambda} \sum_{\alpha=0}^{\alpha=\infty} \frac{1}{N(\lambda)^{\alpha s}} = \Pi^{\lambda} \frac{1}{1-\frac{1}{N(\lambda)^s}} = S.$$

Nun stellt $N(\lambda)$ offenbar folgende reellen Zahlen dar:

1) Die Zahl 3,
2) Die Quadrate aller reellen Primzahlen $3n+2 = Q$,
3) Alle reellen Primzahlen $3n+1 = P$, aber jede *zweimal;* folglich hat man

$$S = \frac{1}{1-\frac{1}{3^s}} \Pi \frac{1}{1-\frac{1}{Q^{2s}}} \left(\Pi \frac{1}{1-\frac{1}{P^s}}\right)^2.$$

Zerlegt man diesen Ausdruck in das Product der beiden Factoren

$$\frac{1}{1-\frac{1}{3^s}}\Pi\frac{1}{1-\frac{1}{Q^s}}\Pi\frac{1}{1-\frac{1}{P^s}} \quad \text{und} \quad \Pi\frac{1}{1+\frac{1}{Q^s}}\Pi\frac{1}{1-\frac{1}{P^s}},$$

so giebt der erste Factor

$$\Pi\frac{1}{1-\frac{1}{L^s}} = \Sigma\frac{1}{M^s},$$

und der zweite

$$\Pi\frac{1}{1-\left(\frac{-3}{L}\right)\frac{1}{L^s}} = \Sigma\left(\frac{-3}{M}\right)\frac{1}{M^s}.$$

Man erhält demnach die Formel

$$\Sigma\frac{1}{N(\mu)^s} = \Sigma\frac{1}{M^s}.\Sigma\left(\frac{-3}{M}\right)\frac{1}{M^s},$$

aus welcher sich, wenn man die beiden Reihen zur Rechten wirklich in einander multiplicirt, der obige Satz unmittelbar ergiebt. Mit Hülfe dieses Satzes zerlegte sich das allgemeine Resultat für die Formen-Anzahl für den speciellen Fall einer reellen Determinante in das Product zweier Reihen, welche genau mit denen zusammenfallen, durch welche nach *Dirichlet* die Formen-Anzahl in der reellen Theorie bestimmt wird. Nachdem nun noch die Gleichung $x^2-\varDelta y^2=1$, deren Fundamental-Auflösung in das allgemeine Resultat eingeht, einer besondern Discussion für diesen speciellen Fall unterworfen worden war, liefsen sich die mitgetheilten Sätze leicht ableiten. Ich bemerke ausdrücklich, um Mifsverständnissen vorzubeugen, dafs unter dem blofsen Worte *Formen-Anzahl,* auf eine *negative* Determinante bezogen, immer nur die Anzahl der *positiven* Formen verstanden ist; also die Anzahlen, wie sie sich im 303ten Artikel der *Disquisitiones arithm.* angegeben finden. Aus den mitgetheilten Sätzen kann man als Corollar noch schliefsen, dafs für jede positive Nichtquadratzahl D das Product der Formen-Anzahlen für die beiden Determinanten D und $-3D$ immer eine *gerade* Zahl ist. Obgleich dieser Satz eine Eigenschaft ausspricht, welche sich nur auf die reellen Formen bezieht, so bedarf es doch des Zusammenwirkens der Hauptsätze in der 5ten Section der *Disquisitiones arithm.*, um ihn durch die Principien der reellen Theorie allein zu beweisen. Es ergiebt sich aus diesen Sätzen, dafs die Anzahl der *Geschlechter (genera)* für jede reelle Determinante, nach den verschiedenen Formen dieser Determinante in Beziehung auf den Modul 8, ent-

weder 2^{m-1}, oder 2^m, oder 2^{m+1} ist (wo für einen Augenblick durch m die Anzahl der in der Determinante aufgehenden verschiedenen ungeraden Primzahlen bezeichnet worden ist), und zwar

2^{m-1}, wenn die Determinante $\equiv 1, 5 \pmod 8$,
2^m, - - - - $\equiv 2, 3, 4, 6, 7 \pmod 8$,
2^{m+1}, - - - - $\equiv 0 \pmod 8$ ist.

Durch Anwendung dieses Resultats auf die beiden Fälle, in welchen die Determinante D und $-3D$ ist, erhält man den in Rede stehenden Satz mit leichter Mühe.

Seit der Zeit, als ich die Untersuchungen hierüber anstellte, habe ich mich auch besonders mit der Theorie der aus 8ten, 16ten, 32sten u. s. w. Wurzeln der Einheit zusammengesetzten complexen Zahlen beschäftigt, welche neue Principien erfordern. Hierbei bin ich in Hinsicht auf die quadratischen Formen zu einer Reihe von Resultaten geführt worden, welche mir sehr merkwürdig zu sein scheinen.

Es bezeichne der Kürze halber $\varphi(D)$ die Anzahl der eigentlich primitiven, nicht-aequivalenten quadratischen Formen mit der Determinante D in der *reellen Theorie*.

Schreiben wir die folgenden vier Formen-Anzahlen

$$\varphi(D), \quad \varphi(-D), \quad \varphi(2D), \quad \varphi(-2D),$$

so hat das Product je zweier, so wie das Product aller vier eine eigenthümliche zahlentheoretische Bedeutung.

Das Product aller vier Anzahlen bestimmt die Formen-Anzahl für die Determinante D in der Theorie der complexen Zahlen aus *achten* Wurzeln der Einheit.

Die beiden Producte $\varphi(D).\varphi(-D)$ und $\varphi(2D).\varphi(-2D)$ geben die Formen-Anzahlen für die Determinanten resp. D und $2D$ in der Theorie der Zahlen $a+b\sqrt{-1}$; wie schon bekannt.

Die beiden Producte $\varphi(D).\varphi(-2D)$ und $\varphi(-D).\varphi(2D)$ geben die Formen-Anzahlen für die Determinanten D und $-D$ in der Theorie der Zahlen von der Form $a+b\sqrt{-2}$.

Endlich finden die beiden Producte $\varphi(D).\varphi(2D)$ und $\varphi(-D).\varphi(-2D)$ ihre Bedeutung in der Theorie der complexen Zahlen $a+b\sqrt{2}$.

Folgender Satz ist allgemeiner.

„Wenn Δ eine aus *vierten* Wurzeln der Einheit zusammengesetzte complexe Zahl ist, so ist die Formen-Anzahl für die Determinante Δ in der

Theorie der aus *achten* Wurzeln der Einheit zusammengesetzten Zahlen bestimmt durch das Product der Formen-Anzahlen für die beiden Determinanten

$$\Delta \quad \text{und} \quad \Delta\sqrt{-1}$$

in der Theorie der aus *vierten* Wurzeln der Einheit zusammengesetzten Zahlen."

Die Art der Abhängigkeit wird für alle diese Sätze durch einfache Criterien angegeben, welche in der Lösbarkeit oder Nichtlösbarkeit gewisser unbestimmter Gleichungen bestehen.

Es existiren ähnliche Sätze, welche einen Zusammenhang zwischen den aus 16ten und den aus 8ten Wurzeln der Einheit zusammengesetzten Zahlen aussprechen; und so weiter.

Die Entscheidung der Frage, ob nicht alle diese Sätze, wie es scheint, als specielle Fälle in einem weit allgemeineren Satze enthalten sind, kann erst von weiteren Untersuchungen erwartet werden; besonders von solchen, die auch die höheren Formen umfassen.

Die allgemeine Bestimmung der Formen-Anzahlen in den Theorieen der aus 8ten, 16ten u. s. w. Wurzeln der Einheit zusammengesetzten Zahlen hangt von einer ganz neuen Gattung von Functionen ab, welche gewissermafsen auf die elliptischen folgen, und von denen wir bereits in den Bemerkungen zu den elliptischen und *Abel*schen Transcendenten Andeutungen gegeben haben.

Im 19ten Bande dieses Journals hat Herr Prof. *Jacobi* bemerkt, dafs sich jede reelle Primzahl von der Form $8n+1$ oder $12n+1$ in das Product aus vier ganzen complexen Primzahlen zerlegen läfst, die resp. aus 8ten und 12ten Wurzeln der Einheit zusammengesetzt sind. Ich bin durch meine Untersuchungen auf zwei Sätze geführt worden, welche nicht allein alle reellen Zahlen bestimmen, die sich auf diese Weise zerlegen lassen, sondern auch die Anzahl der Zerlegungen für jede reelle Zahl ergeben. Um diese Sätze deutlicher und kürzer aussprechen zu können, seien einige Definitionen vorausgeschickt. Für jede aus 8ten oder 12ten Wurzeln der Einheit zusammengesetzte complexe Zahl heifse das Product ihrer vier Werthe das *Normalproduct* der complexen Zahl; eine complexe Einheit heifse jede der unendlich vielen ganzen complexen Zahlen, deren Normalproduct $=+1$ ist; *unähnliche* complexe Zahlen mögen solche genannt werden, welche nicht durch Multiplication mit einer complexen Einheit auseinander entstehen können. Die Sätze lauten dann wie folgt.

„Wenn man eine reelle ganze positive Zahl M auf alle mögliche Arten in ein Product von *vier* reellen Factoren zerlegt, wie

$$M = pqrs,$$

mit der Beschränkung, dafs q, r, s ungerade sein sollen, so giebt die Summe

$$\Sigma\left(\frac{-1}{q}\right)\left(\frac{-2}{r}\right)\left(\frac{2}{s}\right),$$

über alle Combinationen q, r, s ausgedehnt, die Anzahl der unähnlichen, aus 8ten Wurzeln der Einheit zusammengesetzten ganzen complexen Zahlen, welche zu dem Normalproducte M gehören."

„Wenn man eine reelle ganze positive Zahl M auf alle mögliche Arten in ein Product von vier reellen Factoren zerlegt, wie

$$M = pqrs,$$

mit der Beschränkung, dafs q ungerade, r nicht durch 3 theilbar, und s weder durch 2 noch durch 3 theilbar sein soll, so giebt die Summe

$$\Sigma\left(\frac{-1}{q}\right)\left(\frac{-3}{r}\right)\left(\frac{3}{s}\right),$$

über alle Combinationen q, r, s, wie sie so eben definirt wurden, ausgedehnt, die Anzahl der zu demselben Normalproducte M gehörigen unähnlichen, aus 12ten Wurzeln der Einheit zusammengesetzten ganzen complexen Zahlen."

Berlin im März 1844.

23.

Einfacher Algorithmus zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

Wenn p und p_1 irgend zwei ungerade Zahlen ohne gemeinschaftlichen Theiler sind, so bilde man das System von Gleichungen

$$(A.)\quad \begin{cases} p = k p_1 + \varepsilon p_2, \\ p_1 = k_1 p_2 + \varepsilon_1 p_3, \\ p_2 = k_2 p_3 + \varepsilon_2 p_4, \\ \dots\dots\dots\dots \\ p_n = k_n p_{n+1} + \varepsilon_n, \end{cases}$$

wo p, p_1, p_2, p_3 etc. sämmtlich positiv und *ungerade* sind, und wo

$$\varepsilon = \pm 1, \quad \varepsilon_1 = \pm 1, \quad \varepsilon_2 = \pm 1 \text{ etc.},$$

$$p > p_1 > p_2 > p_3 \text{ etc.}$$

ist. Neben jede der so gebildeten Gleichungen

$$p_\mu = k_\mu p_{\mu+1} + \varepsilon_\mu p_{\mu+2}$$

schreibe man als *Randzahl* die *Null*, oder die *Eins*; und zwar die Null, wenn $p_{\mu+1}$ und $\varepsilon_\mu p_{\mu+2}$ entweder beide, oder wenigstens eine dieser beiden Zahlen $\equiv 1$ (mod. 4) ist, die *Eins* dagegen, wenn sowohl $p_{\mu+1} \equiv -1$, als auch $\varepsilon_\mu p_{\mu+2} \equiv -1$ (mod. 4) ist. Die *Summe* aller dieser *Randzahlen* bestimmt dann den Werth von $\left(\frac{p}{p_1}\right)$. Jenachdem nämlich diese Summe *gerade* oder *ungerade* ist, hat man

$$\left(\frac{p}{p_1}\right) = +1 \quad \text{oder} \quad \left(\frac{p}{p_1}\right) = -1.$$

In der That, aus dem obigen System von Gleichungen ergeben sich die folgenden:

$$(B.)\quad \begin{cases} \left(\frac{p}{p_1}\right) = \left(\frac{\varepsilon p_2}{p_1}\right) = (-1)^{\frac{1}{2}(p_1-1)\cdot\frac{1}{2}(\varepsilon p_2-1)}\left(\frac{p_1}{p_2}\right), \\ \left(\frac{p_1}{p_2}\right) = \left(\frac{\varepsilon_1 p_3}{p_2}\right) = (-1)^{\frac{1}{2}(p_2-1)\cdot\frac{1}{2}(\varepsilon_1 p_3-1)}\left(\frac{p_2}{p_3}\right), \\ \left(\frac{p_2}{p_3}\right) = \left(\frac{\varepsilon_2 p_4}{p_3}\right) = (-1)^{\frac{1}{2}(p_3-1)\cdot\frac{1}{2}(\varepsilon_2 p_4-1)}\left(\frac{p_3}{p_4}\right), \\ \dots\dots\dots\dots\dots\dots \\ \left(\frac{p_n}{p_{n+1}}\right) = \left(\frac{\varepsilon_n}{p_{n+1}}\right) = (-1)^{\frac{1}{2}(p_{n+1}-1)\cdot\frac{1}{2}(\varepsilon_n-1)}, \end{cases}$$

und hieraus erhält man durch successive Substitution die Formel

$$\left(\frac{p}{p_1}\right) = (-1)^{\frac{1}{2}(p_1-1)\cdot\frac{1}{2}(\varepsilon p_2-1)+\frac{1}{2}(p_2-1)\cdot\frac{1}{2}(\varepsilon_1 p_3-1)+\dots+\frac{1}{2}(p_{n+1}-1)\cdot\frac{1}{2}(\varepsilon_n-1)},$$

in welcher der Beweis für die Richtigkeit des Satzes liegt.

Aus den Gleichungen (*A.*) findet sich leicht die folgende:

$$\frac{p}{p_1} = k + \cfrac{\varepsilon}{k_1 + \cfrac{\varepsilon_1}{k_2 + \cfrac{\varepsilon_2}{\text{etc.} \atop \ddots \atop k_n + \varepsilon_n}}},$$

und da k, k_1 etc. lauter *gerade* Zahlen sein müssen, so sieht man, dafs die Bestimmung des Werthes von $\left(\frac{p}{p_1}\right)$ auf die Entwicklung von $\frac{p}{p_1}$ in einen Kettenbruch hinauskommt, dessen Zähler von der Form ± 1, und dessen Nenner sämmtlich gerade Zahlen sind.

Beispiel. Es sei der Werth von $\left(\frac{773}{343}\right)$ zu finden. Hier gestaltet sich die Rechnung wie folgt:

```
343|773|2
     686|
     ---|
      87|343|4
         348|
         ---|
          -5| 87|18
              90|
              --|
              -3|  5|2
                   6|
                  --|
                  -1|
```

Man bilde hiernach das System

	Randzahlen.
$773 = 2.343 + 87$	1
$343 = 4.\ 87 - 5$	1
$87 = 18.\ 5 - 3$	0
$5 = 2.\ 3 - 1$	1
Summe der Randzahlen	$= 3$

Also ist

$$\left(\frac{773}{343}\right) = -1.$$

Berlin im Februar 1844.

24.

Eigenschaften und Beziehungen der Ausdrücke, welche bei der Auflösung der allgemeinen cubischen Gleichungen erscheinen.

(Von Herrn Stud. G. *Eisenstein* zu Berlin.)

Als ich im ersten Hefte des 27ten Bandes dieses Journals die allgemeine Auflösung der Gleichungen von den ersten 4 Graden mittheilte, versprach ich, bei einer andern Gelegenheit auf die Eigenschaften der in die Auflösungsformeln eingehenden Ausdrücke zurückzukommen. Vielleicht wird es einigen Lesern nicht unangenehm sein, wenn ich hier dieses Versprechen wenigstens in Beziehung auf die cubischen Gleichungen erfülle.

Die Aufgabe, eine allgemeine cubische Gleichung aufzulösen, ist identisch mit derjenigen, die homogene Function

$$ax^3+3bx^2y+3cxy^2+dy^3 = \Phi$$

in ihre 3 *linearen* Factoren zu zerfällen. Man kann diese Zerfällung auf doppelte Weise ausführen, je nachdem man nämlich in der Gleichung

$$\Phi = 0$$

entweder x oder y als die Unbekannte ansieht. Im ersten Falle findet man, dafs $a^2\Phi$ in das Product dreier Factoren zerfällt, von denen jeder die Form

$$1.\quad ax+\left(b+\sqrt[3]{(\tfrac{1}{2}(a_1+a\sqrt{D}))}+\sqrt[3]{(\tfrac{1}{2}(a_1-a\sqrt{D}))}\right)y$$

hat, und wo die Werthe der Cubikwurzeln so zu nehmen sind, dafs ihr Product

$$= A = b^2-ac$$

wird.

Im zweiten Falle erhält man die Zerlegung von $d^2.\Phi$ in das Product dreier linearer Factoren von der Form

$$2.\quad dy+\left(c+\sqrt[3]{(\tfrac{1}{2}(d_1+d\sqrt{D}))}+\sqrt[3]{(\tfrac{1}{2}(d_1-d\sqrt{D}))}\right)x,$$

wo das Product der Cubikwurzeln

$$= C = c^2-bd$$

sein mufs.

Die Werthe von a_1, d_1, D sind

$$a_1 = a^2 d - 3abc + 2b^3,$$
$$d_1 = d^2 a - 3dcb + 2c^3,$$
$$D = a^2 d^2 - 3b^2 c^2 + 4ac^3 + 4db^3 - 6abcd.$$

Zu den beiden Ausdrücken a_1 und d_1 gesellen sich noch die beiden andern

$$b_1 = abd - 2ac^2 + b^2 c,$$
$$c_1 = dca - 2db^2 + c^2 b,$$

und zu A und C der folgende:

$$B = bc - ad.$$

Diese Ausdrücke von a_1, b_1, c_1, d_1, A, B, C und D bilden zusammen mit den Coëfficienten a, b, c, d ein in sich abgerundetes Ganze.

Wenn man aus den Ausdrücken von $-a_1$, $-b_1$, c_1 und d_1 vier neue auf dieselbe Art entstehen läfst, wie jene aus a, b, c, d entstanden sind, so erhält man resp.

$$-aD^2, \quad -bD^2, \quad -cD^2, \quad -dD^2.$$

Die Ausdrücke a_1, b_1, c_1, d_1 werden aus den *partiellen Differentialquotienten* von D nach d, c, b, a gefunden, wenn man diese letzteren resp. mit

$$\tfrac{1}{2}, \quad -\tfrac{1}{6}, \quad -\tfrac{1}{6} \quad \text{und} \quad \tfrac{1}{2}$$

multiplicirt.

Die drei Formen

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 = \Phi,$$
$$-a_1x^3 - 3b_1x^2y + 3c_1xy^2 + d_1y^3 = \Phi_1,$$
$$Ax^2 + Bxy + Cy^2 = F$$

hangen auf das innigste mit einander zusammen. Wenn man auf alle drei eine lineare Substitution

$$x = \lambda x' + \mu y',$$
$$y = \nu x' + \varrho y',$$

deren Nenner

$$\lambda\varrho - \mu\nu = 1$$

ist, anwendet, so wird man das merkwürdige Verhalten wahrnehmen, dafs zwischen den Coëfficienten der *drei neuen Formen* Φ', Φ_1' und F' in x', y' *genau dieselben* Relationen Statt finden, wie zwischen denen von Φ, Φ_1, F: ein Umstand, der besonders eine wichtige Grundlage für zahlentheoretische Untersuchungen bildet.

Der Ausdruck D, den man *Determinante* von Φ nennen kann, ist zugleich die Determinante von F, weil

$$D = B^2 - 4AC$$

ist. Die Determinante von Φ_1 ist dann D^3. Diese Determinante bleibt bei jeder linearen Substitution, deren Nenner $= 1$ ist, *unverändert*.

Bemerkenswerth sind, aufser mehreren andern, die folgenden identischen Gleichungen:

$$4A^3 = a_1^2 - Da^2, \qquad 4C^3 = d_1^2 - Dd^2,$$
$$A^2 = Ab^2 - Bab + Ca^2,$$
$$AC = Ac^2 - Bbc + Cb^2,$$
$$C^2 = Ad^2 - Bcd + Cc^2,$$
$$Ac - Bb + Ca = Ad - Bc + Cb = 0,$$
$$a_1 = 2Ab - Ba,$$
$$b_1 = Ac - Ca = +2Ac - Bb = +Bb - 2Ca,$$
$$c_1 = -Ad + Cb = -2Ad + Bc = -Bc + 2Cb,$$
$$d_1 = -Bd + 2Cc.$$

Interessant ist noch die Aufgabe, *a posteriori* die *Identität* der beiden Zerlegungen (1.) und (2.) nachzuweisen; was ich dem Leser überlasse.

Berlin, 3. März 1844.

25.

Neuer und elementarer Beweis des Legendreschen Reciprocitäts-Gesetzes.

(Von Herrn Stud. G. *Eisenstein* zu Berlin.)

Nicht leicht möchte die Geschichte eines mathematischen Satzes ein gröfseres Interesse darbieten, als die des berühmten Fundamentaltheorems für die quadratischen Reste. Man weifs, dafs alle Bemühungen der gröfsten Mathematiker vor *Gaufs* an dieser steilen Klippe gescheitert sind, bis es endlich diesem Einzigen gelang, den verborgenen Pfad zu entdecken und bis zum Ziele vorzudringen. Er ist aber auch der Einzige geblieben, der in dieser Hinsicht etwas geleistet hat. Seit einer Reihe von fast dreifsig Jahren ist den sechs Beweisen, welche *Gaufs* von dem Satze gegeben hat, kein neuer hinzugefügt worden; und dies scheint weniger darin seinen Grund gehabt zu haben, dafs man den Gegenstand als abgethan betrachtete, sondern vielmehr in der Schwierigkeit, die sich, selbst nach dem bereits Geleisteten, der Auffindung eines neuen Weges entgegenstellte.

Der neue Beweis, den wir in dieser Abhandlung mittheilen wollen, ist ganz elementarer Art. Er dürfte, aufser der Einfachheit, besonders Das als einen Vorzug in Anspruch nehmen, dafs eine Operation, von deren Ausführbarkeit die Richtigkeit des Satzes abhängt, durch eine rein analytische Transformation allgemein ausführbar gemacht wird.

Wenn nämlich p und q irgend zwei ungerade Primzahlen bezeichnen, und $\left(\frac{q}{p}\right)$ das bekannte Legendresche Zeichen ist, so kommt der ganze Beweis darauf hinaus, die angezeigte Division

$$\frac{(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\cdot p^{\frac{1}{2}(q-1)}-\left(\frac{q}{p}\right)}{q}$$

wirklich auszuführen, d. h. den Dividendus so umzuformen, dafs er in der That durch den Divisor theilbar wird, oder die ganze Zahl $\mathfrak{S}$ allgemein so

zu bestimmen, dafs der Ausdruck ($\varDelta$)

$$(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\cdot p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right) = \mathfrak{G}q \text{ wird.}$$

I. Es seien $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots \alpha_\mu$ allgemeine Glieder der Reihe

$$(\varpi.) \quad 1,\ 2,\ 3,\ \ldots\ldots\ p-1.$$

Man bilde den Ausdruck

$$\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\ldots\left(\frac{\alpha_\mu}{p}\right) = E,$$

dessen Werth offenbar nur die *Einheit* mit dem positiven oder negativen Zeichen sein kann, und bezeichne die Summe

$$2. \quad \Sigma\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\ldots\left(\frac{\alpha_\mu}{p}\right),$$

welche sich über alle Werthe von

$$(\alpha.) \quad \alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots\ldots\ \alpha_\mu$$

erstreckt, durch $\psi(\mu)$. Da diese Summe nichts anders ist als die Potenz

$$\left[\sum_{\sigma=1}^{\sigma=p-1}\left(\frac{\sigma}{p}\right)\right]^\mu,$$

und da $\sum_{\sigma=1}^{\sigma=p-1}\left(\frac{\sigma}{p}\right) = 0$ ist, so hat man

$$3. \quad \psi(\mu) = 0.$$

II. Die Glieder der Summe $\psi(\mu)$ lassen sich in eine Anzahl p von Partialgruppen zerlegen. Da nämlich für jedes Glied E derselben die Summe

$$\alpha_1 + \alpha_2 + \alpha_3 + \ldots\ldots + \alpha_\mu = s$$

einer der p Zahlen $0,\ 1,\ 2,\ \ldots\ldots\ p-1$ nach dem mod. p congruent werden mufs, so rechnen wir in die erste Partialgruppe alle diejenigen Glieder E, für welche $s \equiv 0$ (mod. p) ist; in die zweite Partialgruppe alle diejenigen, für welche $s \equiv 1$ (mod. p) ist, u. s. w.: allgemein, in die $\nu+1$te Partialgruppe alle diejenigen Glieder E, für welche

$$4. \quad \alpha_1 + \alpha_2 + \alpha_3 + \ldots\ldots + \alpha_\mu \equiv \nu \text{ (mod. } p)$$

ist. Wir bezeichnen die p Partialreihen, in welche auf diese Weise $\psi(\mu)$ zerfällt, der Reihe nach durch

$$5. \quad \psi(\mu, 0),\ \psi(\mu, 1),\ \psi(\mu, 2),\ \ldots\ldots\ \psi(\mu, \nu),\ \ldots\ldots\ \psi(\mu, p-1).$$

III. Die Reihen $\psi(\mu,\nu)$ besitzen mehrere merkwürdige Eigenschaften. Man hat zunächst offenbar

$$6. \quad \psi(\mu,0)+\psi(\mu,1)+\ldots+\psi(\mu,p-1) = \psi(\mu) = 0.$$

Ich behaupte ferner, dafs für jeden *nicht durch p theilbaren* Werth von k,

$$7. \quad \psi(\mu,k) = \left(\frac{k}{p}\right)^{\mu} \psi(\mu,1) \text{ ist.}$$

In der That genügt es, in die für $\psi(\mu,k)$ stattfindende Bedingungscongruenz

$$\alpha_1+\alpha_2+\ldots+\alpha_\mu \equiv k \pmod{p}$$

und in das allgemeine Glied der Summe selbst,

$$\alpha_1 \equiv k\beta_1, \quad \alpha_2 \equiv k\beta_2, \quad \ldots\ldots \quad \alpha_\mu \equiv k\beta_\mu \pmod{p}$$

zu substituiren, und zu bedenken, dafs $\beta_1, \beta_2, \ldots \beta_\mu$ dann selbst wieder allgemeine Glieder der Reihe (ω.) werden, um sich von der Richtigkeit der Formel (7.) zu überzeugen. Es ergiebt sich hieraus, dafs für einen *geraden Werth* von μ,

$$8. \quad \psi(\mu,1) = \psi(\mu,2) = \text{etc.} \ldots = \psi(\mu,p-1),$$

also auch, wegen (6.),

$$9. \quad \psi(\mu,0)+(p-1)\psi(\mu,1) = 0 \text{ und}$$

$$10. \quad \psi(\mu,0)-\psi(\mu,1) = -p\psi(\mu,1),$$

dagegen für einen *ungeraden Werth* von μ,

$$11. \quad \psi(\mu,k) = \left(\frac{k}{p}\right)\psi(\mu,1),$$

$$12. \quad \psi(\mu,1)+\psi(\mu,2)+\ldots+\psi(\mu,p-1) = 0 \text{ und}$$

$$13. \quad \psi(\mu,0) = 0 \text{ ist.}$$

IV. Um den Werth der Summen $\psi(\mu,\nu)$ vollständig bestimmen zu können, bilde man eine Recursionsformel, durch welche die Summen $\psi(\mu,\nu)$ in die einfacheren $\psi(\mu-1,\nu)$ ausgedrückt werden.

Man erhält nach der Definition:

$$\psi(\mu,\nu) = \Sigma\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\ldots\left(\frac{\alpha_{\mu-1}}{p}\right)\left(\frac{\alpha_\mu}{p}\right)$$
$$\{\alpha_1+\alpha_2+\ldots+\alpha_{\mu-1}+\alpha_\mu \equiv \nu \pmod{p}\}.$$

Schreibt man das allgemeine Glied E der Summe so:

$$\left(\frac{\alpha_\mu}{p}\right)\times\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\ldots\left(\frac{\alpha_{\mu-1}}{p}\right),$$

und die Bedingungscongruenz so:

$$\alpha_1+\alpha_2+\ldots+\alpha_{\mu-1}\equiv\nu-\alpha_\mu \pmod{p},$$

so zeigt sich auf der Stelle, dafs die Relation

$$14.\quad \psi(\mu,\nu)=\Sigma\left(\frac{\alpha_\mu}{p}\right)\psi(\mu-1,\nu-\alpha_\mu)$$

Statt findet, wo das Σ zur Rechten eine *einfache* Summe anzeigt, die sich auf die Werthe von α_μ bezieht. Es sei, um diese Recursionsformel anzuwenden, zuerst $\nu=0$. Für diesen Fall giebt die Formel

$$\psi(\mu,0)=\Sigma\left(\frac{\alpha_\mu}{p}\right)\psi(\mu-1,-\alpha_\mu).$$

Da $-\alpha_\mu$ nicht durch p theilbar ist, so hat man nach (7.)

$$\psi(\mu-1,-\alpha_\mu)=\left(\frac{-\alpha_\mu}{p}\right)^{\mu-1}\psi(\mu-1,1).$$

Setzt man diesen Werth hinein, so kommt

$$\psi(\mu,0)=\Sigma\left(\frac{-\alpha_\mu}{p}\right)^{\mu}.\left(\frac{-1}{p}\right)\psi(\mu-1,1).$$

Aber $\Sigma\left(\frac{-\alpha_\mu}{p}\right)^{\mu}$ ist offenbar $=p-1$ oder $=0$, je nachdem μ *gerade* oder *ungerade* ist: also erhält man endlich

$$15.\quad \psi(\mu,0)=\left(\frac{-1}{p}\right)(p-1)\psi(\mu-1,1),\ \text{oder}\ =0,$$

je nachdem μ *gerade* oder *ungerade* ist.

Um ebenso $\psi(\mu,k)$ zu bestimmen, wenn k nicht durch p theilbar ist, bemerke ich, dafs für einen *geraden* Werth von μ diese Summe schon durch (15.) mitgegeben ist. In der That, die Formel (9.) giebt

$$\psi(\mu,k)=\frac{-1}{p-1}\psi(\mu,0),$$

also erhält man aus (15.)

$$16.\quad \psi(\mu,k)=-\left(\frac{-1}{p}\right)\psi(\mu-1,1);\quad \mu\ \textit{gerade}.$$

Um endlich den Werth von $\psi(\mu,k)$ auszudrücken, wenn μ *ungerade* ist, bedienen wir uns wieder der Recursionsformel (14.). Sie giebt

$$\psi(\mu,k)=\Sigma\left(\frac{\alpha_\mu}{p}\right)\psi(\mu-1,k-\alpha_\mu).$$

Dasjenige Glied der Reihe zur Rechten, welches dem Werthe $\alpha_\mu=k$ entspricht, liefert $\left(\frac{k}{p}\right)\psi(\mu-1,0)$; für alle übrigen Glieder ist $k-\alpha_\mu$ *nicht*

durch p theilbar, und da $\mu-1$ eine *gerade* Zahl ist, so kann man die Gleichungen (8.) benutzen, und man sieht, dafs alle Glieder der obigen Reihe, mit Ausnahme des schon erhaltenen, gefunden werden, wenn man den gemeinschaftlichen Factor $\psi(\mu-1,1)$ nach und nach mit

$$\left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right),\ \ldots\ \left(\frac{k-1}{p}\right),\ \left(\frac{k+1}{p}\right),\ \ldots\ \left(\frac{p-1}{p}\right)$$

multiplicirt, so dafs sich die Reihe folgendermafsen schreiben läfst:

$$\begin{aligned}\left(\frac{k}{p}\right)\psi(\mu-1,0)+\sum_{\sigma=1}^{\sigma=p-1}\left(\frac{\sigma}{p}\right)\psi(\mu-1,1)-\left(\frac{k}{p}\right)\psi(\mu-1,1)\\ =\left(\frac{k}{p}\right).[\psi(\mu-1,0)-\psi(\mu-1,1)]\\ =-\left(\frac{k}{p}\right)p\psi(\mu-1,1)\ \text{(nach (10.))}.\end{aligned}$$

Wir erhalten also

$$17.\quad \psi(\mu,k)=-\left(\frac{k}{p}\right)p\psi(\mu-1,1);\quad \mu\ \textit{ungerade};$$

und namentlich für $k=1$,

$$18.\quad \psi(\mu,1)=-\left(\frac{-1}{p}\right)\psi(\mu-1,1),\ \text{oder} =-p\psi(\mu-1,1),$$

je nachdem μ *gerade* oder *ungerade* ist.

V. Die Formel (18.) liefert nach und nach das System von Gleichungen

$$\begin{aligned}\psi(2\lambda+1,1)&=-p\psi(2\lambda,1),\\ \psi(2\lambda,1)&=-\left(\frac{-1}{p}\right)\psi(2\lambda-1,1),\\ \psi(2\lambda-1,1)&=-p\psi(2\lambda-2,1),\\ \psi(2\lambda-2,1)&=-\left(\frac{-1}{p}\right)\psi(2\lambda-3,1),\\ &\ldots\ldots\ldots\\ \psi(3,1)&=-p\psi(2,1),\\ \psi(2,1)&=-\left(\frac{-1}{p}\right)\psi(1,1).\end{aligned}$$

Multiplicirt man alle diese Gleichungen mit einander, hebt auf beiden Seiten den gemeinschaftlichen Factor

$$\psi(2\lambda,1)\,\psi(2\lambda-1,1)\ldots\psi(2,1).$$

heraus, und bemerkt, dafs $\psi(1,1)=\left(\frac{1}{p}\right)=1$ und $\left(\frac{-1}{p}\right)=(-1)^{\frac{1}{2}(p-1)}$ ist,

so erhält man

$$19. \quad \psi(2\lambda+1, 1) = (-1)^{\frac{1}{2}(p-1)\cdot\lambda}.p^{\lambda},$$

und hieraus noch nach (18.)

$$20. \quad \psi(2\lambda, 1) = -(-1)^{\frac{1}{2}(p-1)\cdot\lambda}.p^{\lambda-1}.$$

VI. Ist jetzt q eine zweite, von p verschiedene ungerade Primzahl, so hat man nach (19.)

$$21. \quad \psi(q, 1) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.p^{\frac{1}{2}(q-1)}.$$

Wir wollen nun untersuchen, ob in der Summe

$$\psi(q, 1) = \Sigma\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\dots\left(\frac{\alpha_q}{p}\right)$$
$$\{\alpha_1+\alpha_2+\dots+\alpha_q \equiv 1 \pmod{p}\}$$

Glieder vorkommen können, für welche gleichzeitig

$$22. \quad \alpha_1 = \alpha_2 = \alpha_3 = \text{etc.} = \alpha_q \text{ ist.}$$

Diese Bedingungen erfordern die folgende,

$$q\alpha_1 \equiv 1 \pmod{p}:$$

eine Congruenz, welche nur für einen einzigen Werth $\alpha_1 = r$ erfüllt wird. Es existirt also nur ein einziges Glied in $\psi(q, 1)$, für welches alle Elemente α einander gleich sind, und der Werth dieses Gliedes ist

$$\left(\frac{r}{p}\right)^q = \left(\frac{r}{p}\right) = \left(\frac{q}{p}\right).$$

Schliefsen wir dieses Glied von der Summe $\psi(q, 1)$ *aus*, so kommt

$$23. \quad (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right) = \Delta = \Sigma\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\dots\left(\frac{\alpha_q}{p}\right),$$

wo in der Summe zur Rechten $\alpha_1, \alpha_2, \dots \alpha_q$ sämmtlich allgemeine Glieder der Reihe $1, 2, 3, \dots p-1$ vorstellen, und wo alle Combinationen genommen werden müssen, für welche den beiden Bedingungen genügt wird, dafs erstens

$$24. \quad \alpha_1+\alpha_2+\dots+\alpha_q \equiv 1 \pmod{p},$$

und dafs zweitens

25. *nicht gleichzeitig* $\alpha_1 = \alpha_2 = \text{etc.} = \alpha_q$ sei.

Der Ausdruck Δ erscheint hier in der *elementarsten* Weise dargestellt, in welcher man überhaupt eine ganze Zahl zerfällen kann; nämlich als *ein Aggregat von positiven und negativen Einheiten.* Sehen wir jetzt, ob sich unter dieser Form die *Division* durch die Primzahl q wird verrichten lassen.

VII. Es sei

$$\alpha_1 = m_1, \quad \alpha_2 = m_2, \quad \ldots\ldots \quad \alpha_q = m_q$$

irgend ein System von Werthen, welches den Bedingungen genügt, denen die Elemente α in (24.) und (25.) unterworfen sind, so dafs

$$26. \qquad m_1 + m_2 + \ldots\ldots + m_q \equiv 1 \pmod{p},$$

$$27. \qquad \textit{und dafs nicht zugleich} \quad m_1 = m_2 = \text{etc.} = m_q.$$

Dann genügen offenbar die folgenden q Systeme, welche durch cyclische Permutation der Elemente aus einander entstehen und von denen das erste das vorgelegte ist, nemlich

$$28. \qquad \begin{cases} m_1, & m_2, & m_3, & \ldots\ldots & m_{q-1}, & m_q, \\ m_2, & m_3, & m_4, & \ldots\ldots & m_q, & m_1, \\ m_3, & m_4, & m_5, & \ldots\ldots & m_1, & m_2, \\ \cdot & \cdot & \cdot & \cdot\cdot\cdot\cdot & \cdot & \cdot \\ m_q, & m_1, & m_2, & \ldots\ldots & m_{q-2}, & m_{q-1}, \end{cases}$$

allen den Bedingungen (24.) und (25.); wie unmittelbar aus der symmetrischen Natur von (26.) und (27.) in Beziehung auf ihre Elemente klar ist. Diese q Systeme sind alle von einander *verschieden*, weil q eine Primzahl ist und *nicht* alle Elemente einander gleich sind; sie ertheilen aber dem allgemeinen Gliede der Summe (23.) alle genau *denselben* Werth. Es folgt hieraus, dafs die Totalsumme (23.) in eine Anzahl von Gruppen getheilt werden kann, so dafs jede Gruppe q *einander gleiche* Glieder enthält; und somit ist die Theilbarkeit unseres Ausdrucks Δ durch q erwiesen. Es ist leicht, hiernach den Quotienten selbst hinzuschreiben. Derselbe ist

$$29. \qquad \frac{(-1)^{\frac12(p-1)\cdot\frac12(q-1)}\, p^{\frac12(q-1)} - \left(\frac{q}{p}\right)}{q} = \mathfrak{S} = \Sigma\left(\frac{\alpha_1}{p}\right)\left(\frac{\alpha_2}{p}\right)\ldots\left(\frac{\alpha_q}{q}\right);$$

wo sich die Summe über alle Werthe der verschiedenen α erstreckt, welche den in (24.) und (25.) ausgesprochenen Bedingungen genügen, wo aber noch die Beschränkung hinzutritt, dafs von je q Systemen, welche auseinander durch *cyclische* Permutation der Elemente wie in (28.) entstehen, immer *nur ein einziges* genommen werden mufs.

VIII. Das Legendresche Reciprocitätsgesetz ist eine unmittelbare Folgerung der eben veranstalteten Umformung. In der That, wie eben gezeigt wurde, ist

$$(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\, p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right) \text{ durch } q \text{ theilbar;}$$

aufserdem ist aber

$$p^{\frac{1}{2}(q-1)} \equiv \left(\frac{p}{q}\right) \pmod{q},$$

folglich ist auch

$$(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \left(\frac{p}{q}\right) - \left(\frac{q}{p}\right)$$

durch q theilbar, was nicht anders geschehen kann, als wenn

$$30.\quad \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \left(\frac{q}{p}\right)$$

ist; was zu beweisen war.

Berlin im April 1844.

26.

Encyklopädische und elementare Darstellung der Theorie der Zahlen.

(Vom Herausgeber dieses Journals.)

(Fortsetzung der Abhandlung No. 2. im 1sten und No. 10. im 2ten Hefte dieses Bandes.)

---

§. 43.

Erklärung.

In den gewöhnlichen algebraischen Gleichungen von der Form

$$1. \quad \varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} + \varepsilon_{n-3} x^{n-3} \ldots + \varepsilon_1 x + \varepsilon_0 = 0,$$

wo der Exponent n eine *ganze positive* Zahl ist und die ε beliebige Zahlgröfsen sind, kann bekanntlich x nur n von einander verschiedene, positive oder negative, reelle oder imaginäre *Werthe* haben, und diese Werthe von x nennt man *Wurzeln* der Gleichung.

In der Theorie der Zahlen kommen Gleichungen vor, die ganz dieselbe *Form* wie die algebraischen (1.) haben, nur dafs zu dem letzten Gliede noch ein *unbestimmtes* Vielfache irgend einer *bestimmten* Zahl z hinzugethan oder davon hinweggenommen ist, während zugleich alle Coëfficienten ε positive oder negative *ganze* Zahlen sind: Gleichungen also, welche die Form

$$2. \quad \varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} + \varepsilon_{n-3} x^{n-3} \ldots + \varepsilon_1 x + \varepsilon_0 = \mathfrak{G} z$$

haben Solche Gleichungen drücken, wie man sieht, aus, dafs das *Polynom* oder die *Potenzenreihe* linkerhand mit der bestimmten Zahl z *aufgehe.* Für solche Gleichungen kommt es dann insbesondere auf diejenigen positiven oder negativen *ganzzahligen* Werthe von x an, welche die eben genannte Bedingung erfüllen, oder welche der Gleichung (2.) *genugthun.* Diese ganzzahligen Werthe von x nennt man ebenfalls *Wurzeln* der Gleichung (2.). Sie sollten zwar, bestimmter, *ganzzahlige Wurzeln* der Gleiehung heifsen, aber da in der Zahlentheorie überhaupt nur von *ganzen* Zahlen die Rede ist, so kann das Beiwort *ganzzahlig* auch füglich wegbleiben und man kann die der Gleichung (2.) genugthuenden ganzzahligen Werthe von x blofs *Wurzeln* nennen. Gleichungen wie (2.) kann man dagegen, wenn man will, zum Unterschiede von den gewöhnlichen algebraischen Gleichungen, wie (1.), *Zahlengleichungen* nennen.

§. 44.

Lehrsatz.

I. *Die Zahlengleichung*

$$1. \quad f_n x = \varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots + \varepsilon_2 x^2 + \varepsilon_1 x + \varepsilon_0 = \mathfrak{G} p,$$

in welcher der Zeiger n *an* f *den* ***Grad*** *des Polynoms oder der Potenzenreihe* $\varepsilon_n x^n + \varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots + \varepsilon_0$ *bezeichnet, kann, wenn* p *eine* ***Stammzahl*** *ist, und* ε_n *und* ε_0 *gehen* ***nicht*** *mit p auf,* ***nicht mehr*** *als* n ***positive*** *ganzzahlige Wurzeln* $x > 0$ *und* $< p$ *haben; gleichviel ob andere von den* ε *als* ε_n *und* ε_0 *mit p aufgehen, oder nicht.*

II. *Gehen die ersten* x *Coëfficienten* $\varepsilon_n, \varepsilon_{n-1}, \varepsilon_{n-2}, \ldots \varepsilon_{n-x+1}$ *mit* p *auf, der nächste Coëfficient* ε_{n-x}, *nebst* ε_0 *aber nicht, so kann die Gleichung* (1.) ***nicht mehr*** *als* $n-x$ *positive ganzzahlige Wurzeln* >0 *und* $<$ p *haben; gleichviel ob andere* ε *mit* p *aufgehen, oder nicht.*

III. *Gehen die* ***letzten*** λ *Coëfficienten* $\varepsilon_{\lambda-1}, \varepsilon_{\lambda-2}, \varepsilon_{\lambda-3}, \ldots \varepsilon_0$ *mit* p *auf, der nächst vorige Coëfficient* ε_λ *nebst* ε_n *aber nicht, so hat die Gleichung* (1.) *zunächst nothwendig* p *zur Wurzel; aufserdem aber kann sie* ***nicht mehr*** *als* $n-\lambda$ *positive ganzzahlige Wurzeln* >0 *und* $<$ p *haben; gleichviel ob andere* ε *mit* p *aufgehen, oder nicht.*

IV, *Gehen die ersten* x *und die letzten* λ *Coëfficienten* (II. u. III.) *mit* p *auf, der nächste Coëfficient* ε_{n-x} *links und der nächste Coëfficient* ε_λ *rechts aber nicht, so hat die Gleichung* (1.) *erst nothwendig* p *zur Wurzel; aufserdem kann sie* ***nicht mehr*** *als* $n-x-\lambda$ ***positive*** *ganzzahlige Wurzeln* >0 *und* $<$ p *haben; gleichviel ob andere* ε *mit* p *aufgehen, oder nicht.*

V. *Jedesmal hat die Gleichung* (1.) *auch noch* ***eben soviele negative*** *ganzzahlige Wurzeln, deren Werth zeichenfrei* >0 *und* $<$p *ist, als sie* ***positive*** *Wurzeln hat. Diese negativen Wurzeln finden sich, wenn man von den positiven Wurzeln* p *abzieht.*

VI. ***Nur dann,*** *wenn* ***alle*** *Coëfficienten* ε *einzeln mit* p *aufgehen, kann die Gleichung* (1.) ***mehr*** *als* n *positive und* n *negative ganzzahlige Wurzeln haben, deren Werthe zeichenfrei* >0 *und* $<$ p *sind; und zwar hat sie dann nothwendig* ***alle*** *die Zahlen* $\pm(1, 2, 3, 4, \ldots p-1)$ *zu Wurzeln.*

VII. *Keinesweges aber hat die Gleichung* (1.) ***nothwendig*** *immer* n *positive und* n *negative Wurzeln* >0 *und* $<$p. *Sie kann deren auch weniger, und selbst gar keine haben.*

VIII. *Ist* $n=p$, *oder* $>p$, *so kann die Gleichung* (1.) *alle die Zahlen* $\pm(1, 2, 3, 4, \ldots p-1)$ *zu Wurzeln haben; jedoch auch* ***nicht*** *alle, und selbst* ***keine*** *derselben.*

IX. *Soll* $f_n x$ *auch* ***nur für einen*** *mehr als* n *Werthe von* $x>0$

und $<$ p *mit* p *aufgehen: soll also die Gleichung* (1.) *auch nur für einen mehr als* n *solcher Werthe von* x *erfüllt werden, so ist dies nicht anders möglich, als dafs alle die Coëfficienten* ε *einzeln mit* p *aufgehen.*

X. *Wenn die Gleichung* (1.) *nicht* n, *sondern nur* $k < n$ *Wurzeln* > 0 *und* $< p$ *hat, also das Polynom* $f_n x$ *nur für* k *Werthe von* x > 0 *und* $< p$ *aufgeht, so läfst sich die Gleichung* $f_n x = \mathfrak{G} p$ (1.) *immer auf die Form*

$$2.\quad f_n x = (x-e_1)(x-e_2)(x-e_3)\ldots(x-e_k)\, f_{n-k} x = \mathfrak{G} p$$

bringen, wo $e, e_1, e_3, \ldots e_k$ *die* k *Werthe* > 0 *und* $< p$ *sind, für welche* $f_n x$ *mit* p *aufgeht,* $f_{n-k} x$ *aber ein Polynom vom Grade* $n-k$ *ist, welches* ε_n *zum Coëfficienten seines ersten Gliedes, also* $\varepsilon_n x^{n-k}$ *zum ersten Gliede hat und, insofern* $n-k > 1$, *für keinen der andern Werthe von* x *mit* p *aufgeht.*

Auch pafst der Ausdruck (2.) *von* $f_n x$ *gleichmäfsig auf den Fall, wenn die Gleichung* (1.) n *Wurzeln hat oder* $f_n x$ *für* n *Werthe von* x > 0 *und* $< p$ *mit* p *aufgeht. Es ist alsdann* $k = n$; *in* (2.) *ist* $f_{n-k} x = \varepsilon_n$ *und der Ausdruck von* (1.) *also alsdann*

$$3.\quad f_n x = (x-e_1)(x-e_2)(x-e_3)\ldots(x-e_n)\varepsilon_n = \mathfrak{G} p.$$

XI. *Wenn in* (1.) ε_n *nicht mit* p *aufgeht, aber auch nur dann, läfst sich die Gleichung* (1.), *wenn das Polynom für* k *Werthe von* x > 0 *und* $< p$ *mit* p *aufgeht, immer auf eine andere*

$$4.\quad f_n x = (x^k - \delta_{k-1} x^{k-1} + \delta_{k-2} x^{k-2} - \delta_{k-3} x^{k-3} \ldots \mp \delta_2 x^2 \pm \delta_1 x \mp \delta_0) f_{n-k} x = \mathfrak{G} p$$

bringen, in welcher das erste Glied des Polynoms vom Grade k, 1 *zum Coëfficienten hat, das erste Glied des für keinen Werth von* x *mit* p *aufgehenden Factors* $f_{n-k} x$, $\varepsilon_n x^{n-k}$ *ist, und die* δ *der Reihe nach die Summen der Producte der* k *Werthe* $e_1, e_2, e_3, \ldots e_k$ *von* x $> 0 < p$ *zu einem, zweien, dreien etc. bis* k *sind, für welche* $f_n x$ *mit* p *aufgeht.*

In dem Fall, wo $f_n x$ *für* n *Werthe von* x > 0 *und* $< p$ *mit* p *aufgeht, läfst sich die Gleichung* (1.) *auf die Form*

$$5.\quad f_n x = (x^n - \delta_{n-1} x^{n-1} + \delta_{n-2} x^{n-2} - \delta_{n-3} x^{n-3} \ldots \mp \delta_2 x^2 \pm \delta_1 x \mp \delta_0)\varepsilon_n = \mathfrak{G} p$$

bringen, wo wiederum das erste Glied des Polynoms vom Grade n, 1 *zum Coëfficienten hat und die* δ *der Reihe nach die Summen der Producte der* n *Werthe* $e_1, e_2, e_3, \ldots e_n$ *von* x $> 0 < p$ *zu einem, zweien, dreien etc. bis* n *sind, für welche* $f_n x$ *mit* p *aufgeht.*

Immer gehen die Producte $(x-e_1)(x-e_2)(x-e_3)\ldots(x-e_k)$ *in* (2.) *und* $(x-e_1)(x-e_2)(x-e_3)\ldots(x-e_n)$ *in* (3.), *ersteres für die nemlichen*

k, *letzteres für die nemlichen* n *Werthe von* x *mit* p *auf, wie das Polynom* $f_n x$ *selbst. Und eben so verhält es sich mit den Polynomen von den Graden* k *und* n *in* (4. und 5.).

XII. *Wenn ein Polynom* $f_n x$ *für* $n-1$ *Werthe von* $x > 0 < p$ *aufgeht, so geht es auch noch für einen* nten *Werth von* $x > 0 < p$ *mit* p *auf, der aber nicht nothwendig von einem der Werthe* $e_1, e_2, e_3, \ldots e_{n-1}$ *verschieden ist.*

Beispiele. *a.* 1. Die Gleichung

$$6.\quad x^3+2x^2+x-4 = \mathfrak{G}.11,$$

für welche $n=3$, $p=11$ ist, hat $n=3$ positive und eben so viele negative Wurzeln. Jene sind $+1$, $+3$ und $+5$, diese -1, -8 und -6. Denn für alle diese Werthe von x geht x^3+2x^2+x-4 mit $p=11$ auf.

2. Die Gleichung

$$7.\quad 2x^4-5x^3-26x^2+4x-9 = \mathfrak{G}.7,$$

für welche $n=4$, $p=7$ ist, hat nur die $k=2$ positiven Wurzeln 4 und 5 und die $k=2$ negativen Wurzeln -3 und -2. Für keinen andern Werth von $x<p=7$ geht $2x^4-5x^3-26x^2+4x-9$ mit $p=7$ auf.

3. Die Gleichung

$$8.\quad 3x^3-16x^2+25x+58 = \mathfrak{G}.7,$$

für welche $n=3$, $p=7$ ist, hat wieder die $n=3$ positiven Wurzeln $+1$, $+3$ und $+6$ und die $n=3$ negativen Wurzeln -6, -4 und -1.

4. Die Gleichung

$$9.\quad 4x^3-8x^2-2x+9 = \mathfrak{G}.7$$

hat *gar keine* ganzzahligen Wurzeln.

5. Die Gleichung

$$10.\quad x^6-1 = \mathfrak{G}.7$$

hat alle die Zahlen $\pm(1, 2, 3, 4, 5 \text{ und } 6=(p-1))$ zu Wurzeln.

b. Die Gleichung (7.) ist das Nemliche wie

$$11.\quad (x-4)(x-5)(2x^2+13x+51) = \mathfrak{G}.7-203x+1029$$
$$= 7(\mathfrak{G}-29x+147) = \mathfrak{G}.7,$$

wo der Factor $f_2 x = 2x^2+13x+51$ für *keinen* Werth $>0 <p$ von x mit p aufgeht und das erste Glied dieses Factors $2x^2 = \varepsilon_n x^{n-k}$ ist; gemäfs (2.).

Die Gleichung (8.) ist das Nemliche wie

$$12.\quad (x-1)(x-3)(x-6).3 = \mathfrak{G}.7-14x^2+56x+112$$
$$= 7(\mathfrak{G}+2x^2+8x+16) = \mathfrak{G}.7,$$

wo der Factor 3 von $(x-1)(x-3)(x-6)$ gleich ε_n ist; gemäfs (3.).

c. Die Ausdrücke (11.) und (12.) sind so viel als

$$13.\quad (x^2-9x+20)(2x^2+13x+51) = \mathfrak{G}.7 \quad \text{und}$$

$$14.\quad (x^3-10x^2+27x-18).3 = \mathfrak{G}.7.$$

In (13.) ist, mit (4.) verglichen, $\delta_{k-1}=9=4+5$, $\delta_{k-2}=\delta_0=20=4.5$. In (14.) ist, mit (5.) verglichen, $\delta_{n-1}=10=1+3+6$, $\delta_{n-2}=27=1.3+1.6+3.6$ und $\delta_{n-3}=\delta_0=18=1.3.6$; gemäfs (X.).

Beweis. *A.* Es werde das Polynom $f_n x$ durch das *Binom* $x-e_1$ *dividirt*, so wird das erste Glied des Quotienten $\varepsilon_n x^{n-1}$, und der Quotient wird ein Polynom vom Grade $n-1$ sein, also durch $f_{n-1}x$ bezeichnet werden können; der *Rest* der Division, welcher r_1 sein mag, wird *gar kein* x enthalten, weil man mit der Division so lange fortfahren kann, als ein Glied des Rests noch x enthält. Die Division giebt nemlich Folgendes:

$$15.\quad x-e_1 \mid \varepsilon_n x^n + \varepsilon_{n-1}x^{n-1}+\varepsilon_{n-2}x^{n-2}+\varepsilon_{n-3}x^{n-3}\ldots+\varepsilon_1 x+\varepsilon_0 \mid \varepsilon_n x^{n-1}+(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-2}$$

$$-\varepsilon_n x^n+e_1\varepsilon_n x^{n-1} \qquad\qquad +(\varepsilon_{n-2}+e_1\varepsilon_{n-1}+e_1^2\varepsilon_n)x^{n-3}\ldots$$

$$\overline{(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-1}+\varepsilon_{n-2}x^{n-2}+\varepsilon_{n-3}x^{n-3}\ldots+\varepsilon_1 x+\varepsilon_0}$$

$$-(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-1}+e_1(\varepsilon_{n-1}+e_1\varepsilon_n)x^{n-2}$$

$$\overline{(\varepsilon_{n-2}+e_1\varepsilon_{n-1}+e_1^2\varepsilon_n)x^{n-2}+\varepsilon_{n-3}x^{n-3}\ldots+\varepsilon_1 x+x_0}$$

Und so weiter.

Man wird also setzen können:

$$16.\quad f_n x = (x-e_1)f_{n-1}x+r_1,$$

wo von $f_{n-1}x$ das *erste* Glied $\varepsilon_n x^{n-1}$ ist und r_1 *kein* x enthält.

B. Das Polynom $f_{n-1}x$ in (16.) vom Grade $n-1$ werde nun von neuem durch ein anderes *Binom* $x-e_2$ dividirt, so wird man aus ganz gleichen Gründen setzen können:

$$17.\quad f_{n-1}x = (x-e_2)f_{n-2}x+r_2,$$

wo das *erste* Glied von $f_{n-2}x$ wieder $\varepsilon_n x^{n-2}$ ist und r_2 *kein* x enthält.

Ferner wird man setzen können, wenn weiter das Polynom $f_{n-2}x$ vom Grade $n-2$ in (17.) mit einem dritten *Binom* $x-e_3$ dividirt wird:

$$18.\quad f_{n-2}x = (x-e_3)f_{n-3}x+r_3,$$

wo von $f_{n-3}x$ das *erste Glied* $\varepsilon_n x^{n-3}$ ist und r_3 kein x enthält.

Und so weiter; zuletzt also

$$19.\quad f_1 x = (x-e_n)f_0 x+r_n,$$

wo das *erste Glied* von $f_0 x$, das heifst $f_0 x$ selbst ist, weil $f_0 x$ vom Grade 0 ist, also *nur ein* Glied hat und nur $x^0=1$ vorkommt, $=\varepsilon_n x^0=\varepsilon_n$ ist und r_n kein x enthält.

C. Es sind nemlich, wie aus (15.) zu sehen, die Polynome $f_{n-1}x$, $f_{n-2}x$, $f_{n-3}x$, ... der Reihe nach von der Form

$$20.\quad \begin{cases} f_{n-1}x = \varepsilon_n x^{n-1} + \overset{1}{\varepsilon}_{n-2} x^{n-2} + \overset{1}{\varepsilon}_{n-3} x^{n-3} \dots + \overset{1}{\varepsilon}_1 x + \overset{1}{\varepsilon}_0, \\ f_{n-2}x = \varepsilon_n x^{n-2} + \overset{2}{\varepsilon}_{n-3} x^{n-3} + \overset{2}{\varepsilon}_{n-4} x^{n-4} \dots + \overset{2}{\varepsilon}_1 x + \overset{2}{\varepsilon}_0, \\ f_{n-3}x = \varepsilon_n x^{n-3} + \overset{3}{\varepsilon}_{n-4} x^{n-4} + \overset{3}{\varepsilon}_{n-5} x^{n-5} \dots + \overset{3}{\varepsilon}_1 x + \overset{3}{\varepsilon}_0, \\ \dots\dots\dots\dots\dots\dots \end{cases}$$

Geht man also damit bis zum vorletzten Polynom vom Grade $n-(n-1)=1$ fort, so wird solches die Form

$$21.\quad f_1 x = \varepsilon_n x + \overset{n-1}{\varepsilon}_0$$

bekommen, und dieses, mit dem letzten Binom $x-e_n$ dividirt, giebt

$$22.\quad f_1 x = \varepsilon_n(x-e_n) + \varepsilon_n e_n + \overset{n-1}{\varepsilon}_0,$$

welches, mit (19.) verglichen,

$$23.\quad f_0 x = \varepsilon_n \text{ und}$$

$$24.\quad \varepsilon_n e_n + \overset{n-1}{\varepsilon}_0 = r_n$$

giebt; letzteres ohne x.

D. Substituirt man nun zunächst (17.) in (16.), so ergiebt sich

$$25.\quad f_n x = (x-e_1)(x-e_2) f_{n-2} x + (x-e_1) r_2 + r_1.$$

Substituirt man hierin (18.), so erhält man

$$26.\quad f_n x = (x-e_1)(x-e_2)(x-e_3) f_{n-3} x + (x-e_1)(x-e_2) r_3 + (x-e_1) r_2 + r_1,$$

u. s. w.; zuletzt, da $f_0 = \varepsilon_n$ ist,

$$27.\quad \begin{aligned} f_n x = {} & (x-e_1)(x-e_2)(x-e_3)\dots(x-e_n)\varepsilon_n \\ & + (x-e_1)(x-e_2)(x-e_3)\dots(x-e_{n-1}) r_n \\ & + (x-e_1)(x-e_2)(x-e_3)\dots(x-e_{n-2}) r_{n-1} \\ & + (x-e_1)(x-e_2)(x-e_3)\dots(x-e_{n-3}) r_{n-2} \\ & \dots\dots\dots\dots\dots\dots \\ & + (x-e_1)(x-e_2) r_3 \\ & + (x-e_1) r_2 \\ & + r_1. \end{aligned}$$

E. Ist nun e_1 einer der ***ganzzahligen positiven*** Werthe von $x < p$ und > 0, welche der Gleichung (1.) genugthun, so giebt der Ausdruck von $f_n x$ (27.) für $x = e_1$, da alle Glieder rechts bis auf das letzte $x - e_1$ zum Factor haben und also für $x = e_1$ verschwinden,

$$28.\quad f_n e_1 = r_1;$$

und da nun zugleich gemäfs (1.) $f_n e_1 = \mathfrak{G}p$ sein soll,

$$29. \quad r_1 = \mathfrak{G}p.$$

F. Ist e_2 ein zweiter der *ganzzahligen positiven* Werthe von $x > 0$ und $< p$, welche der Gleichung (1.) genugthun, so giebt der Ausdruck (27.) für $x = e_2$, da alle Glieder rechts bis auf die beiden letzten $x - e_2$ zum Factor haben und also für $x = e_2$ verschwinden,

$$30. \quad f_n e_2 = (e_2 - e_1) r_2 + r_1,$$

und da $f_n e_2$ gemäfs (1.) $= \mathfrak{G}p$ sein soll und r_1 nach (29.) schon $= \mathfrak{G}p$ ist,

$$31. \quad (e_2 - e_1) r_2 = \mathfrak{G}p.$$

Nun sind aber e_1 und e_2 beide $< p$ und positiv, also ist auch der zeichenfreie Werth von $e_2 - e < p$, und folglich geht $e_2 - e_1$ *nicht* mit p auf. Daher mufs, vermöge (31.) und (§. 25.), r_2 mit p aufgehen und folglich

$$32. \quad r_2 = \mathfrak{G}p$$

sein.

G. Ist e_3 ein dritter der *ganzzahligen positiven* Werthe von $x > 0$ und $< p$, welche der Gleichung (1.) genugthun, so giebt der Ausdruck (27.) für $x = e_3$, da alle Glieder rechts bis auf die drei letzten für $x = e_3$ verschwinden,

$$33. \quad f_n e_3 = (e_3 - e_1)(e_3 - e_2) r_3 + (e_3 - e_1) r_2 + r_1,$$

und da $f_n e_3$ gemäfs (1.) $= \mathfrak{G}p$ sein soll und r_1 und r_2 gemäfs (29. und 32.) ebenfalls $= \mathfrak{G}p$ sind,

$$34. \quad (e_3 - e_1)(e_3 - e_2) r_3 = \mathfrak{G}p.$$

Hier geht wieder weder $e_3 - e_1$ noch $e_3 - e_2$ mit p auf, weil e_1, e_2, e_3 sämmtlich $< p$ und positiv sind: also mufs r_3 mit p aufgehen und folglich

$$35. \quad r_3 = \mathfrak{G}p \text{ sein.}$$

So findet sich weiter $r_4 = \mathfrak{G}p$, $r_5 = \mathfrak{G}p$ etc., und zusammen

$$36. \quad r_1,\ r_2,\ r_3,\ r_4,\ \ldots\ r_n = \mathfrak{G}p,$$

wenn $e_1, e_2, e_3, \ldots e_n$, n verschiedene ganzzahlige Werthe von $x > 0$ und $< p$ sind, die der Gleichung (1.) genugthun.

H. Da nun die Gleichung (27.) für *jeden beliebigen* Werth von x, so wie für *beliebige* Werthe der e Statt findet, indem der Ausdruck von $f_n x$ rechts eine blofse, durch die wiederholte Division entstandene *identisch* verwandelte Form von $f_n x$ ist, wo, wie sich so eben fand, *in dem Fall* wo die e die n verschiedenen Werthe von x, > 0 und $< p$ bezeichnen, für welche $f_n x$ mit p der Voraussetzung nach *aufgeht,* die sämmtlichen r gleich $\mathfrak{G}p$ sein *müssen,* so giebt die Gleichung (27.) für diesen Fall:

37. $f_n x = (x-e_1)(x-e_2)(x-e_3)\ldots.(x-e_n)\varepsilon_n + \mathfrak{G}p$,

für ***jeden beliebigen*** Werth von x.

I. Hieraus folgt nun, dafs $f_n x$ für ***nicht mehr*** als n Werthe von x, die >0 und $<p$ sind, mit p aufgehen kann, insofern nicht ε_n mit p aufgeht. Denn gesetzt es sei zu den n Werthen $e_1, e_2, e_3, \ldots. e_n$ von x, >0 und $<p$, für welche $f_n x$ nach der Voraussetzung mit p aufgeht, k noch ein $n+1$ter solcher Werth, also $f_n k = \mathfrak{G}p$, so müfste vermöge (37.)

38. $(k-e_1)(k-e_2)(k-e_3)\ldots.(k-e_n)\varepsilon_n = \mathfrak{G}p$

sein. Dies aber ist nicht möglich, da $e_1, e_2, e_3, \ldots. e_n$ und k sämmtlich >0 und $<p$ sein sollen, also auch die zeichenfrei genommenen Werthe aller der Factoren $k-e_1$, $k-e_2$, $k-k_3$, ... $k-e_k$, $<p$ sind, desgleichen ε_n nach der Voraussetzung nicht mit p aufgeht. Also ist es in dem so eben genannten Fall von ε_n nicht möglich, dafs $f_n x$ für ***mehr*** als n Werthe von x, die >0 und $<p$ sind, mit p aufgehe, oder dafs die Gleichung (1.) in diesem Falle mehr als n positive ganzzahlige Wurzeln >0 und $<p$ habe. Und zwar ist es gleichgültig, ob die Coëfficienten $\varepsilon_{n-1}, \varepsilon_{n-2}, \varepsilon_{n-3}, \ldots. \varepsilon_1$ mit p aufgehen, oder nicht; denn sie kommen in der Gleichung (24.), aus welcher das Nicht-Stattfinden von mehr als n positiven Wurzeln der Gleichung (1.) folgt, nicht vor. Dieses zusammen ist was (I.) behauptet.

K. Geht ε_n mit p ***auf***, so ist $\varepsilon_n x^n = \mathfrak{G}p$, für ***jeden*** Werth von x. Eben so sind, wenn etwa weiter $\varepsilon_{n-1}, \varepsilon_{n-2}, \varepsilon_{n-3}$ u. s. w. bis ε_{n-x+1} mit p aufgehen, und dann zunächst ε_{n-x} ***nicht***, auch alle die Glieder $\varepsilon_{n-1}x^{n-1}$, $\varepsilon_{n-2}x^{n-2}$, $\varepsilon_{n-3}x^{n-3}$, ... $\varepsilon_{n-x+1}x^{n-x+1}$ gleich $\mathfrak{G}p$; was auch x sein mag. Also reducirt sich die Gleichung (1.) in diesem Fall auf

39. $\varepsilon_{n-x}x^{n-x} + \varepsilon_{n-x-1}x^{n-x-1} + \varepsilon_{n-x-2}x^{n-x-2}\ldots. + \varepsilon_1 x + \varepsilon_0 = \mathfrak{G}p$;

und diese Gleichung kann nach (I.) ***nicht mehr*** als $n-x$ positive ganzzahlige Wurzeln >0 und $<p$ haben, gleichviel ob andere von den auf ε_{n-x} ***folgenden*** Coëfficienten, den letzten ausgenommen, mit p aufgehen, oder nicht. Gemäfs (II.).

L. Gehen $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots. \varepsilon_{\lambda-1}$ mit p auf, so sind alle die Glieder ε_0, $\varepsilon_1 x$, $\varepsilon_2 x^2$, $\varepsilon_3 x^3$, ... $\varepsilon_{\lambda-1}x^{\lambda-1}$ gleich $\mathfrak{G}p$; was auch x sein mag. Also reducirt sich die Gleichung (1.) in diesem Fall auf

$\varepsilon_n x^n + \varepsilon_{n-1}x^{n-1} + \varepsilon_{n-2}x^{n-2}\ldots. + \varepsilon_\lambda x^\lambda = \mathfrak{G}p$ oder

40. $x^\lambda(\varepsilon_n x^{n-\lambda} + \varepsilon_{n-1}x^{n-\lambda-1} + \varepsilon_{n-2}x^{n-\lambda-2}\ldots. + \varepsilon_{\lambda+1}x + \varepsilon_\lambda) = \mathfrak{G}p$.

Dieser Gleichung wird offenbar zunächst für $x=p$ genuggethan; sodann aber kann der Factor zu x^λ zufolge (I.) für ***nicht mehr*** als $n-\lambda$ Werthe von x,

>0 und $<p$, mit p aufgehen. Also kann die Gleichung (1.) in solchem Falle nur $n-\lambda$ solcher Wurzeln haben, während sie aufserdem ***nothwendig*** p selbst zur Wurzel hat. Gemäfs (III.). Zugleich folgt hieraus, dafs es für (I.) eine ***Bedingung*** ist, dafs der letzte Coëfficient ε_0 ***nicht*** mit p aufgehe; denn ist dies der Fall, so modificirt sich (I.) nach (III.).

M. Gehen die ersten $\varkappa$ und die letzten λ Coëfficienten ε mit p auf, so sind alle die Glieder, in welchen sich diese Coëfficienten befinden, gleich $\mathfrak{G}p$; was auch x sein mag. Also reducirt sich die Gleichung in diesem Fall auf

$$\varepsilon_{n-\varkappa}x^{n-\varkappa}+\varepsilon_{n-\varkappa-1}x^{n-\varkappa-1}+\varepsilon_{n-\varkappa-2}x^{n-\varkappa-2}\ldots+\varepsilon_\lambda x^\lambda=\mathfrak{G}p \text{ oder}$$

$$41. \quad x^\lambda(\varepsilon_{n-\varkappa}x^{n-\varkappa-\lambda}+\varepsilon_{n-\varkappa-1}x^{n-\varkappa-\lambda-1}+\varepsilon_{n-\varkappa-2}x^{n-\varkappa-\lambda-2}\ldots+\varepsilon_{\lambda+1}x+\varepsilon_\lambda)=\mathfrak{G}p.$$

Dieser Gleichung wird wieder zunächst für $x=p$ genuggethan; sodann aber kann der Factor zu x^λ zufolge (I.) für ***nicht mehr*** als $n-\varkappa-\lambda$ Werthe von x, >0 und $<p$, mit p aufgehen. Also kann die Gleichung (1.) in dem gegenwärtigen Falle nur $n-\varkappa-\lambda$ solcher Wurzeln haben, während sie aufserdem ***nothwendig*** p selbst zur Wurzel hat. Gemäfs (IV.).

N. Wenn $f_n x$ (1.) für $x=e$ mit p aufgeht, so geht es auch nothwendig für $x=e-p$ mit p auf. Denn $x=e-p$ ist so viel als $x=\mathfrak{G}p+e$, und zufolge (§. 11. 20.) ist alsdann, für jeden beliebigen ganzzahligen positiven Exponenten τ,

$$42. \quad x^\tau=\mathfrak{G}p+e^\tau;$$

also giebt (1.), wenn man darin $e-p$ statt x setzt, vermöge (29.),

$$f_n(e-p)=\mathfrak{G}p+\varepsilon_n e^n+\varepsilon_{n-1}e^{n-1}+\varepsilon_{n-2}e^{n-2}\ldots+\varepsilon_2 e^2+\varepsilon_1 e+\varepsilon_0 \text{ oder}$$

$$43. \quad f_n(e-p)=\mathfrak{G}p+f_n e.$$

Ist also $f_n e=\mathfrak{G}p$, so ist es auch $f_n(e-p)$, und folglich gehört zu ***jeder positiven*** ganzzahligen Wurzel $e>0$ und $<p$, welche die Gleichung (1.) hat, auch eine ***negative*** ganzzahlige Wurzel $e-p$, deren zeichenfreier Werth ebenfalls >0 und $<p$ ist. Gemäfs (V.).

O. Gehen ***alle*** Coëfficienten ε in (1.) einzeln mit p auf, so ist ***jedes*** Glied von $f_n x$ gleich $\mathfrak{G}p$ und folglich die ***ganze*** Potenzenreihe $f_n x=\mathfrak{G}p$; und dieser Gleichung thut ***jeder beliebige*** Werth von x ein Genüge. Also hat alsdann die Gleichung (1.) alle die Zahlen $\pm(1,2,3,4,\ldots p-1)$, deren absoluten Werthe >0 und $<p$ sind, zu Wurzeln. Jedoch ist es so auch ***nur*** in dem vorausgesetzten Fall; sind nicht ***alle*** ε gleich $\mathfrak{G}p$, so verhält es sich nach den verschiedenen Umständen gemäfs (I. II. III. oder IV.). Dieses behauptet (VI.).

P. Um nachzuweisen, dafs zufolge (VII.) die Gleichung (1.) auch ***weniger*** als n ganzzahlige Wurzeln > 0 und $< p$ haben kann, darf nur gezeigt werden, dafs es in ***irgend einem*** Falle sich so verhalte. Auf einen solchen Fall führt der Fermatsche Lehrsatz (§. 40.). Diesem Satze zufolge nemlich hat die Gleichung

$$44. \quad x^{p-1} - 1 = \mathfrak{G}p$$

alle die Zahlen 1, 2, 3, 4, ... $p - 1$ zu Wurzeln. ***Eben deshalb*** aber hat z. B. die Gleichung

$$45. \quad x^{p-1} - 2 = \mathfrak{G}p \quad \text{oder} \quad x^{p-1} - 1 - 1 = \mathfrak{G}p$$

keine der Zahlen 1, 2, 3, 4, ... $p - 1$ zu Wurzeln, und folglich ***gar keine*** Wurzeln; denn da $x^{p-1} - 1$ für $x = 1, 2, 3, 4, \ldots . p - 1$ mit p aufgeht, und 1 ***nicht,*** so geht $x^{p-1} - 1 - 1$ oder $x^{p-1} - 2$ für ***keine*** der Werthe 1, 2, 3, ... $p - 1$ von x mit p auf, und folglich hat (32.) ***gar keine*** Wurzeln.

Q. Der Beweis von (I.) ändert sich nicht, wenn auch $n = p$ oder $> p$ ist. Also könnte in diesem Fall die Gleichung (1.) n verschiedene Wurzeln > 0 und $< p$ haben. Aber es ***giebt nur*** die $p - 1$ Zahlen $1, 2, 3, \ldots . p - 1$, welche > 0 und $< p$ sind; also kann die Gleichung (1.) in solchem Fall alle die Zahlen $\pm(1, 2, 3, 4, \ldots . p - 1)$ zu Wurzeln haben; wiewohl auch nicht alle, und selbst keine derselben. Gemäfs (VIII.).

R. Wenn $f_n x$ für n verschiedene Werthe von $x > 0 < p$ aufgeht, so verwandelt sich $f_n x$ zufolge (*H.*) in den Ausdruck (37.). Derselbe kann zufolge (*I.* 38.) nicht anders für einen $n + 1$ten Werth von x mit p aufgehen, als wenn ε_n mit p aufgeht. Also mufs, schon wenn $f_n x$ auch nur für einen mehr als die n Werthe $e_1, e_2, e_3, \ldots . e_n$ von x mit p aufgehen soll, nothwendig ε_n mit p aufgehen.

Geht nun aber ε_n mit p auf, so ist das ***erste Glied*** $\varepsilon_n x^n$ von $f_n x$ (1.) selbst $= \mathfrak{G}p$ und das Polynom $f_n x$ reducirt sich auf ein anderes $\varepsilon_{n-1} x^{n-1} + \varepsilon_{n-2} x^{n-2} \ldots . + \varepsilon_0$ vom $n - 1$ten Grade. Dieses kann schon selbst für n Werthe, und um so mehr für $n + 1$ Werthe von x, aus ***demselben*** Grunde nicht anders mit p aufgehen, als wenn ε_{n-1} mit p aufgeht. Dadurch, dafs ε_{n-1} mit p aufgehen mufs, reducirt sich dann das Polynom weiter auf ein anderes $\varepsilon_{n-2} x^{n-2} + \varepsilon_{n-3} x^{n-3} \ldots . + \varepsilon_0$ vom $n - 2$ten Grade; und hier mufs wieder $\varepsilon_{n-2} = \mathfrak{G}p$ sein u. s. w.; bis zu $\varepsilon_0 = \mathfrak{G}p$ Also müssen, wie es (IX.) behauptet, wenn $f_n x$ für mehr als n Werthe von $x > 0 < p$ mit p aufgehen soll, alle die Coëfficienten ε in (1.) einzeln mit p aufgehen.

S. Um zu beweisen was (X.) behauptet, dividire man zuerst, eben

wie in (15.), $f_n x$ durch $x-e_1$, hierauf, wie dort in (16.), $f_{n-1}x$ durch $x-e_2$, $f_{n-2}x$ wie in (17.) durch $x-e_3$ u. s. w., fahre aber damit nicht wie in (*B.* und *C.*) bis zu $x-e_n$ fort, so dafs die letzte Gleichung nicht die (19.) ist, sondern nur bis zu $x-e_k$, so dafs die letzte Gleichung

$$46.\quad f_{n-k+1}x = (x-e_k)f_{n-k}x + r_k$$

ist, wo indessen immer wie in (16, 17, 18.) das erste Glied von $f_{n-k}x$ $\varepsilon_n x^{n-k}$ ist und r_k *kein* x enthält.

T. Substituirt man nun wieder erst (17.) in (16.), in das Resultat (18.), u. s. w., so wird man, ähnlich dem Ausdruck (27.), für welchen $k=3$ sein würde,

$$\begin{aligned} 47.\quad f_n x = & (x-e_1)(x-e_2)(x-e_3)\dots(x-e_k)f_{n-k}x \\ & +(x-e_1)(x-e_2)(x-e_3)\dots(x-e_{k-1})r_k \\ & +(x-e_1)(x-e_2)(x-e_3)\dots(x-e_{k-2})r_{k-1} \\ & +(x-e_1)(x-e_2)(x-e_3)\dots(x-e_{k-3})r_{k-2} \\ & \dots\dots\dots\dots\dots\dots \\ & +(x-e_1)(x-e_2)r_3 \\ & +(x-e_1)r_2 \\ & +r_1 \end{aligned}$$

erhalten.

U. Ist nun e_1 einer der ganzzahligen positiven Werthe von $x>0$ $<p$, welche der Gleichung (1.) genugthun, so giebt (47.), für $x=e_1$,

$$48.\quad f_n x_1 = r_1,$$

und da $f_n e_1 = \mathfrak{G}p$ sein soll,

$$49.\quad r_1 = \mathfrak{G}p.$$

Ist e_2 ein zweiter Werth von x, für welchen $f_n e_2 = \mathfrak{G}p$ ist, so giebt (47.) für $x=e_2$

$$50.\quad f_n e_2 = (e_2-e_1)r_2 + r_1 = \mathfrak{G}p,$$

oder, da r_1 schon $=\mathfrak{G}p$ ist (49.),

$$51.\quad (e_2-e_1)r_2 = \mathfrak{G}p,$$

und da e_2-e_1 mit p *nicht* aufgeht (*F.*),

$$52.\quad r_2 = \mathfrak{G}p.$$

Ist e_3 ein dritter Werth von x, für welchen $f_n x_3 = \mathfrak{G}p$ ist, so giebt (47.) für $x=e_3$

$$53.\quad f_n e_3 = (e_3-e_1)(e_2-1)r_3 + (e_3-e_1)x_2 + r_1 = \mathfrak{G}p,$$

oder, da r_1 und r_2 schon $=\mathfrak{G}p$ sind (49. und 52.),

$$54.\quad (e_3-e_1)(e_2-e_1)r_3 = \mathfrak{G}p,$$



also, da $e_3 - e_1$ und $e_2 - e_1$ *nicht* mit p aufgehn,

$$55. \quad r_3 = \mathfrak{G}p.$$

Und so weiter.

So findet man aus (47.), bis zu r_k, dafs

$$56. \quad r_1, r_2, r_3, \ldots r_k = \mathfrak{G}p$$

und also vermöge (47.)

$$57. \quad f_n x = (x-e_1)(x-e_2)(x-e_3)\ldots(x-e_k) f_{n-k} x + \mathfrak{G}p$$

ist.

V. Hier geht rechterhand die Gröfse $(x-e_1)(x-e_2)\ldots(x-e_k)f_{n-k}x$ offenbar für $x = e_1, e_2, e_3, \ldots e_k$ mit p auf, eben wie es von $f_n x$ selbst vorausgesetzt wird; denn für jeden dieser Werthe von x ist sie $=0$. Also ist im Fall $f_n x$ für $x = e_1, e_2, e_3, \ldots e_k$ mit p aufgeht:

58. $(x-e_1)(x-e_2)(x-e_3)\ldots(x-e_k)f_{n-k}x = \mathfrak{G}p$, gemäfs (2.), eben wie es $f_n x = \mathfrak{G}p$ ist (1.); und auf diese Form kann also in solchem Fall die Gleichung (1.) gebracht werden.

Das erste Glied von $f_{n-k}x$ ist $\varepsilon_n x^{n-k}$, gemäfs (*S.*); auch kann $f_{n-k}x$, insofern $n-k > 1$ ist, für keinen andern Werth von x mehr mit p aufgehen, denn sonst müfste vermöge (57.) $f_n x$ selbst für einen solchen Werth von x mit p aufgehen, gegen die Voraussetzung; gemäfs (IX.).

W. Der Ausdruck (3.) in (X.) geht unmittelbar aus (2.) oder (58.) hervor, wenn man $k = n$ setzt, und pafst auf den Fall, wenn $f_n x$ für n Werthe von $x > 0 < p$ mit p aufgeht.

X. Zufolge (§. 2.) ist

$$59. \quad (1+a)(1+b)(1+c)\ldots(1+k) = 1 + P_1 + P_2 + P_3 \ldots + P_k,$$

wenn man durch $P_1, P_2, P_3, \ldots P_k$ die Summe aller möglichen Producte der Gröfsen $a, b, c, \ldots k$ zu einer, zwei, drei etc. bis k bezeichnet.

Man setze in (59.)

$$60. \quad a = -\frac{e_1}{x}, \quad b = -\frac{e_2}{x}, \quad c = -\frac{e_3}{x}, \quad \ldots \quad k = -\frac{e_k}{x}$$

und multiplicire (59.) rechts und links mit x^k, so erhält man

$$x^k\left(1-\frac{e_1}{x}\right)\left(1-\frac{e_2}{x}\right)\left(1-\frac{e_3}{x}\right)\ldots\left(1-\frac{e_k}{x}\right) = x^k(1+P_1+P_2+P_3\ldots+P_k)$$

oder

$$61. \quad (x-e_1)(x-e_2)(x-e_3)\ldots(x-e_k) = x^k + x^k P_1 + x^k P_2 + x^k P_3 \ldots + x^k P_k.$$

Hier bedeuten die P die Summen aller möglichen Producte von $-\frac{e_1}{x}$, $-\frac{e_2}{x}$, $-\frac{e_3}{x}$, $\ldots -\frac{e_k}{x}$ zu einem, zwei, drei etc., bis k. Die Producte dieser

sämmtlich ***negativen*** Gröfsen werden vom ersten ab abwechselnd negativ und positiv sein und der Reihe nach x, x^2, x^3, ... x^k im Nenner enthalten. Es werden also die P, wenn man der Reihe nach die Summen aller möglichen Producte der Gröfsen e_1, e_2, e_3, ... e_k selbst, wie in (X. zu 4.), durch δ_{k-1}, δ_{k-2}, δ_{k-3}, ... δ_0 bezeichnet, folgende Werthe haben:

$$62.\quad P_1 = -\frac{\delta_{k-1}}{x},\quad P_2 = -\frac{\delta_{k-2}}{x^2},\quad P_3 = -\frac{\delta_{k-3}}{x^3},\quad \ldots\ldots\quad P_k = -\frac{\delta_0}{x^k}.$$

Diese Ausdrücke in (61.) gesetzt, giebt

$$63.\quad (x-e_1)(x-e_2)(x-e_3)\ldots\ldots(x-e_k)$$
$$= x^k - \delta_{k-1}x^{k-1} + \delta_{k-2}x^{k-2} - \delta_{k-3}x^{k-3} \ldots\ldots \pm \delta_0,$$

und dies weiter in (2.) substituirt, giebt den Ausdruck (4.) des Lehrsatzes.

Der Ausdruck (5.) geht unmittelbar aus (4.) hervor, für $k = n$.

Y. Wenn $f_n x$ für $k = n-1$ Werthe von $x > 0 < p$ aufgeht, so ist in seinem Ausdrucke (2.) $n-k=1$, also $f_{n-k}x$ von der Form $\varepsilon_n x + \beta$, oder, wenn man $\varepsilon_n = \mathfrak{G}p + a$ und $\beta = \mathfrak{G}p + b$ setzt, von der Form $(\mathfrak{G}p + a)x + \mathfrak{G}p + b = \mathfrak{G}p + ax + b$, wo a und $b > 0 < p$ sind. Und $ax + b$ geht ***immer*** für irgend ein $x > 0 < p$ mit p auf. Denn zu $ax + b = \mathfrak{G}p$ gehört, da ε_n, und folglich a zu p theilerfremd ist, immer nach (§. 34.) ***ein*** solcher Werth von $x > 0 < p$. Also geht $f_{n-k}x$ immer noch für irgend einen Werth von $x > 0 < p$, der aber nicht nothwendig von e_1, e_2, e_3, ... e_{n-1} verschieden ist, mit p auf, und folglich auch in (2.) $f_n x$; gemäfs (XII.).

Z. Der gegenwärtige Lehrsatz findet wieder vielfältige weitere Anwendungen und ist daher wieder einer der Hauptlehrsätze der Zahlentheorie.

§. 45.

Lehrsatz.

Wenn in der Gleichung

$$1.\quad (mp+z)^2 = \mathfrak{G}p + r$$

p ***eine ungerade Stammzahl*** > 2 ***ist und man giebt dem positiven oder negativen*** z ***die zeichenfreien Werthe***

$$2.\quad 1, 2, 3, 4, \ldots\ldots p-1,$$

so dafs mp+z, ***mit beliebigem ganzzahligem*** m, ***alle möglichen positiven oder negativen, mit*** p ***nicht aufgehenden ganzen Zahlen ausdrückt, so durchläuft***

I. ***wenn man für ein gleiches*** m ***der Reihe nach***

$$3.\quad z = +1, +2, +3, +4, \ldots\ldots +p-1,$$
$$4.\quad z = -1, -2, -3, -4, \ldots\ldots -(p-1)$$

setzt, der absolute Werth von r *in* (1.) *niemals etwa ebenfalls* ***alle*** *die Zahlen* (2.), *sondern* ***immer*** *nur* ***die Hälfte*** *derselben, und immer die* ***nemlichen,*** *was auch* m *sein mag; die andere Hälfte der Zahlen* (2.) *wird von* r *für das* ***gleiche*** p *niemals berührt. Auch geben schon*

$$5. \quad z = \pm 1,\ \pm 2,\ \pm 3,\ \ldots\ \pm \tfrac{1}{2}(p-1)$$

alle *Werthe von* r *welche Statt finden; die folgenden*

$$6. \quad z \pm \tfrac{1}{2}(p-1)+1,\ \tfrac{1}{2}(p-1)+2,\ \tfrac{1}{2}(p-1)+3,\ \ldots\ p-1$$

geben ***dieselben*** r, *und zwar in* ***entgegengesetzter*** *Aufeinanderfolge. Desgleichen geben positive und negative* z *von gleichen absoluten Werthen gleiche* r.

II. *Da in* (1.) r *nichts anders ist als der* ***Rest,*** *welcher bleibt, wenn man das* ***Quadrat*** $(mp+z)^2$ *mit* p ***dividirt,*** *so ist* r *ein* ***Rest zu einem Quadrat*** *oder ein* ***Quadratrest.*** *Und da nun nach* (1.) *die Hälfte der Zahlen* (2.) *von* r *berührt wird, so sind diese Hälfte der Zahlen* (2.) ***Quadratreste zu*** p; *die andere Hälfte, welche* r *nicht berührt, sind* ***nicht*** *Reste von Quadraten, also* ***Nicht-Quadratreste*** *zu* p.

III. *Da man die Gleichung* (1.) *auch, mit einem* ***ganz beliebigen*** *positiven oder negativen ganzzahligen* n, *wie folgt schreiben kann:*

$$7. \quad (mp+z)^2 = \mathfrak{S}p+(np+r) = \mathfrak{S}p+R,$$

indem nur $\mathfrak{S}$ *in* (7.) *um* n *kleiner sein darf, als in* (1.), *so kann in* (7.) *auch*

$$8. \quad np+r = R$$

als der ***Rest*** *der Division des Quadrats* $(mp+z)^2$ *durch* p *betrachtet werden, und folglich als* ***Quadratrest*** *zu* p. *Da aber* n ***ganz beliebig*** *ist, so kann die Zahl* R *positiv oder negativ und so grofs oder so klein gemacht werden, als man will. Und da nun* r *nach* (I.) *immer nur* ***die Hälfte*** *der Zahlen* (2.) *berührt, so giebt es überhaupt eben so viele mit* p *nicht aufgehende Zahlen, die durch* R (6.) *ausgedrückt werden, als dergleichen Zahlen, die* R *nicht ausdrückt.*

In Folge dessen ist denn ***jede mögliche*** *positive oder negative ganze, grofse oder kleine, nicht mit* p *aufgehende Zahl entweder* ***Quadratrest*** *oder* ***Nichtquadratrest*** *zu* p, *und für jedes* n *sind eben so viele Zahlen* ***Quadratreste,*** *als andere* ***Nichtquadratreste.***

Die R *für* $n=0$, *oder die* r, *deren absolute Werthe unter den Zahlen* (2.) *sich befinden, und die also* >0 *und* $<p$ *sind, könnte man zum Unterschiede von den gröfsern oder kleinern* R *positive oder negative* ***echte*** *Quadratreste und die Hälfte der Zahlen* (2.), *welche von* (2.)

nicht berührt werden, positive oder negative echte Nichtquadratreste nennen.

Beispiel 1. Es sei

$$9. \qquad p = 7,$$

so ist in (7.) der Reihe nach für $m = 0, 1, 2, 3, \ldots$, $n = 0, 1, 2, 3, \ldots$ und $z = \pm(1, 2, 3, \ldots)$

$$10. \left\{ \begin{array}{rlll} (0p\pm1)^2 & = +\ 0p+1 & = -\ 1p+\ 8 & = -\ 2p+15\ldots \\ & = +\ 1p-6 & = +\ 2p-13 & = +\ 3p-20\ldots \\ (0p\pm2)^2 & = +\ 0p+4 & = -\ 1p+11 & = -\ 2p+18\ldots \\ & = +\ 1p-3 & = +\ 2p-10 & = +\ 3p-17\ldots \\ (0p\pm3)^2 & = +\ 1p+2 & = -\ 0p+\ 9 & = -\ 1p+16\ldots \\ & = +\ 2p-5 & = +\ 3p-12 & = +\ 4p-19\ldots \\ (0p\pm4)^2 & = +\ 2p+2 & = +\ 1p+\ 9 & = +\ 0p+16\ldots \\ & = +\ 3p-5 & = +\ 4p-12 & = +\ 5p-19\ldots \\ (0p\pm5)^2 & = +\ 3p+4 & = +\ 2p+11 & = +\ 1p+18\ldots \\ & = +\ 4p-3 & = +\ 5p-10 & = +\ 6p-17\ldots \\ (0p\pm6)^2 & = +\ 5p+1 & = +\ 4p+\ 8 & = +\ 3p+15\ldots \\ & = +\ 6p-6 & = +\ 7p-13 & = +\ 8p-20\ldots \\ (\pm1p\pm1)^2 & = +\ 9p+1 & = +\ 8p+\ 8 & = +\ 7p+15\ldots \\ & = +10p-6 & = +19p-13 & = +12p-20\ldots \\ (\pm1p\pm2)^2 & = +11p+4 & = +10p+11 & = +\ 9p+18\ldots \\ & = -12p-3 & = +11p-10 & = +10p-17\ldots \\ \ldots & \ldots & \ldots & \ldots \end{array} \right.$$

Die *positiven echten* Quadratreste sind hier 1, 4, 2, die *negativen echten* Quadratreste -6, -3 und -5, und die einen und die andern ergeben sich schon aus $z = \pm(1, 2, 3)$, also aus der *ersten Hälfte* der Werthe von $z = \pm(1, 2, 3, 4, 5, 6)$. Dieselben positiven und negativen echten Reste kehren für $(\pm 1p \pm z)^2$, $(\pm 2p \pm z)^2$ etc. immer wieder. Die Zahlen 3, 5 und 6 aus (2.) werden hier von den positiven echten Resten und die Zahlen 1, 2 und 4 von den negativen echten Resten nicht berührt. Erstere sind also die *positiven echten Nichtquadratreste,* letztere die *negativen echten Nichtquadratreste* zu $p = 7$. Überhaupt sind

$$11. \left\{ \begin{array}{l} \text{die positiven Zahlen } +(1, 2, 4, 8, 9, 11, 15, 16, 18, \ldots) \\ \text{und die negativen Zahlen } -(3, 5, 6, 10, 12, 13, 17, 19, 20, \ldots) \end{array} \right\} \textit{Quadratreste} \text{ zu } p = 7 \text{ und}$$

$$12. \left\{ \begin{array}{l} \text{die positiven Zahlen } +(3, 5, 6, 10, 12, 13, 17, 19, 20, \ldots) \\ \text{und die negativen Zahlen } -(1, 2, 4, 8, 9, 11, 15, 16, 18, \ldots) \end{array} \right\} \textit{Nichtquadratreste} \text{ zu } p = 7.$$

2. Da es insbesondere auf die *echten* positiven und negativen Quadratreste und Nichtquadratreste ankommt, so setzen wir dieselben vorläufig für einige der ersten ungeraden Stammzahlen >2 hierher. Die echten positiven und die negativen echten Quadratreste bezeichnen wir durch $\pm r$, und die echten positiven und negativen Nichtquadratreste durch $\pm \varrho$.

$$
13.\quad \left\{ \begin{array}{ll}
\text{Für } p=3 \text{ ist} & +r=+1,\quad +\varrho=+2, \\
& -r=-2,\quad -\varrho=-1; \\
\text{Für } p=5 \text{ ist} & +r=+(1,4),\quad +\varrho=+(2,3), \\
& -r=-(1,4),\quad -\varrho=-(2,3); \\
\text{Für } p=7 \text{ ist} & +r=+(1,2,4),\quad +\varrho=+(3,5,6), \\
& -r=-(3,5,6),\quad -\varrho=-(1,2,4); \\
\text{Für } p=11 \text{ ist} & +r=+(1,3,4,5,\ 9),\quad +\varrho=+(2,6,7,8,10); \\
& -r=-(2,6,7,8,10),\quad -\varrho=-(1,3,4,5,\ 9); \\
\text{Für } p=13 \text{ ist} & +r=+(1,3,4,9,10,12),\quad +\varrho=+(2,5,6,7,8,11), \\
& -r=-(1,3,4,9,10,12),\quad -\varrho=-(2,5,6,7,8,11); \\
\text{Für } p=17 \text{ ist} & +r=+(1,2,4,8,9,13,15,16), \\
& \qquad +\varrho=+(3,5,6,7,10,11,12,14), \\
& -r=-(1,2,4,8,9,13,15,16), \\
& \qquad -\varrho=-(3,5,6,7,10,11,12,14); \\
\text{Für } p=19 \text{ ist} & +r=+(1,4,5,\ 6,\ 7,\ 9,11,16,17), \\
& \qquad +\varrho=+(2,3,8,10,12,13,14,15,18), \\
& -r=-(2,3,8,10,12,13,14,15,18), \\
& \qquad -\varrho=-(1,4,5,\ 6,\ 7,\ 9,11,16,17); \\
\text{Für } p=23 \text{ ist} & +r=+(1,2,\ 3,\ 4,\ 6,\ 8,\ 9,12,13,16,18), \\
& \qquad +\varrho=+(5,7,10,11,14,15,17,19,20,21,22), \\
& -r=-(5,7,10,11,14,15,17,19,20,21,22), \\
& \qquad -\varrho=-(1,2,\ 3,\ 4,\ 6,\ 8,\ 9,12,13,16,18); \\
\text{Für } p=29 \text{ ist} & +r=+(1,4,5,6,7,9,13,16,20,22,23,24,25,28), \\
& +\varrho=+(2,3,8,10,11,12,14,15,17,18,19,21,26,27), \\
& -r=-(1,4,5,6,7,9,13,16,20,22,23,24,25,28), \\
& -\varrho=-(2,3,8,10,11,12,14,15,17,18,19,21,26,27); \\
\text{Für } p=31 \text{ ist} & +r=+(1,2,\ 4,\ 5,\ 7,\ 8,\ 9,10,14,16,18,19,20,25,28), \\
& +\varrho=+(3,6,11,12,13,15,17,21,22,23,24,26,27,29,30), \\
& -r=-(3,6,11,12,13,15,17,21,22,23,24,26,27,29,30), \\
& -\varrho=-(1,2,\ 4,\ 5,\ 7,\ 8,\ 9,10,14,16,18,19,20,25,28); \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array} \right.
$$

Beweis *A*. Es ist $(-z)^2 = +z^2$. Also geben positive und negative z von gleichem absolutem Werthe *gleiche* Reste r.

B. Es ist $(p-z)^2 = p^2 - 2pz + z^2 = \mathfrak{G}p + z^2$, also ist

14. wenn $z^2 = \mathfrak{G}p + r$ ist, auch $(p-z)^2 = \mathfrak{G}p + r$.

Also geben z^2 und $(p-z)^2$ *gleiche* Reste r. Setzt man daher

15. $z = \pm(1, 2, 3, \ldots \frac{1}{2}(p-1)$,

so geben sie *denselben* Rest r wie

16. $z = \pm(p-1, p-2, p-3, \ldots \frac{1}{2}(p+1))$,

und folglich giebt schon die *erste Hälfte* der Zahlen $\pm(1, 2, 3, \ldots p-1)$ *alle* Quadratreste r; die *zweite Hälfte* giebt *dieselben* Reste, und zwar in *umgekehrter* Aufeinanderfolge: denn $p-1$ giebt denselben Rest wie 1, $p-2$ denselben Rest wie 2 u. s. w.

Dieses zusammen ist was in (I.) behauptet wird. Das Übrige ist an sich klar.

Anm. *C*. Die Benennungen *quadratische und nichtquadratische Reste zu* p, welche man hie und da auch findet, dürfte grammatisch weniger richtig sein als *Quadratreste* und *Nichtquadratreste*, welches geradezu ausdrückt, was gemeint ist; denn jene Benennung würde Reste bezeichnen, die *selber Quadrate* oder nicht Quadrate, oder doch quadratischer oder nicht quadratischer Art sind; was hier nicht der Fall ist, indem die r keinesweges *immer Quadrate*, und eben so wenig die Zahlen, welche r nicht berührt, nothwendig immer *nicht Quadrate* sind.

§. 46.

Erklärung.

Zwei ganze Zahlen z_1 und z_2, deren Product, durch eine dritte ganze Zahl a dividirt, den Rest r giebt, so dafs

1. $z_1 z_2 = \mathfrak{G}a + r$

ist, nennt man, wenn mehrere solcher Zahlenpaare zu *demselben* Divisor a *denselben* Rest r geben, *correspondirende* oder auch *conjugirte* Zahlen.

Da die Zahlen z_1 und z_2 in (1.) nichts anders sind als Factoren von $\mathfrak{G}a +$ dem Rest r, oder einfacher, ein *Factorenpaar für r zu a*, so könnten sie auch füglich *so heifsen*. Will man indessen eine andere, nicht unmittelbar bezeichnende, sondern nur mehr andeutende Benennung, so könnte man die Zahlen z_1 und z_2 *auf Deutsch zusammengehörige Zahlen* nennen; doch müfste dann der Unterscheidung wegen eigentlich noch hinzugesetzt werden „für r zu a."

§. 47.

Lehrsatz.

I. *Wenn* p *eine* ***ungerade Stammzahl*** *ist, so sind alle die Zahlen*

$$1.\quad z = 2, 3, 4, 5, \dots\, p-2$$

je zu zweien ***Factorenpaare*** *von* 1 *zu* a *(zusammengehörige Zahlen für* 1 *zu* p §. 46.), *so dafs in*

$$2.\quad z_1 z_2 = \mathfrak{G}p+1$$

z_1 *und* z_2 *alle die Zahlen* (1.) *sein können. Und zwar ist in* (2.) *für keins der* z, (1.) z_1 *gleich* z_2. *Auch gehört zu jedem* z_1 ***nur ein*** z_2, *so dafs in* (2.) z_1 *und* z_2 ***jeden*** *der Werthe von* z (1.) ***nur einmal*** *haben können. Die* ***Anzahl*** *der* ***Factorenpaare*** *ist* $\frac{1}{2}(p-3)$.

II. *Die beiden von den Zahlen* $<p$ *noch übrigen Zahlen* 1 *und* $p-1$ *geben mit keinem der* z (1.), *sondern nur* ***mit sich selbst*** *multiplicirt* $\mathfrak{G}p+1$, *und* ***mit einander*** *multiplicirt,*

$$3.\quad 1.(p-1) = \mathfrak{G}p-1.$$

III. *Wenn in*

$$4.\quad z_1 z_2 = \mathfrak{G}p+\varrho$$

ϱ *ein positiver* ***Nichtquadratrest*** (§. 45. II.) *ist, so sind* ***alle*** *Zahlen* $<p$, *also* ***alle*** *die Zahlen*

$$5.\quad z = 1, 2, 3, 4, \dots\, p-1$$

je zu zweien ***Factorenpaare*** *von* ϱ *zu* p *(zusammengehörige Zahlen für* ϱ *zu* p §. 46.), *so dafs in*

$$6.\quad z_1 z_2 = \mathfrak{G}p+\varrho$$

z_1 *und* z_2 *alle die Zahlen* (5.) *sein können. Und zwar kann wieder in* (6.) *für kein* z (5.) z_1 ***gleich*** z_2 *sein. Auch gehört zu jedem* z_1 ***nur ein*** z_2, *so dafs in* (6.) z_1 *und* z_2 *jeden der Werthe von* z (5.) ***nur einmal*** *haben können. Die* ***Anzahl*** *der* ***Factorenpaare*** *ist hier* $\frac{1}{2}(p-1)$.

Beispiel. Zu I. und II. Es sei $p=13$, so sind 2.7; 3.9; 4.10; 5.8 und 6.11 sämmtlich $=\mathfrak{G}p+1$. Keiner der Factoren in diesen $\frac{1}{2}(p-3)$ $=5$ Producten ist dem andern *gleich;* keiner kommt mehr als einmal vor, und die Factoren durchlaufen *alle* die Zahlen 2, 3, 4, 5, 6, 7, 8, 9, 10 und $11=p-2$ (1.); gemäfs (I.). Die Gleichung (3.) in (II.) ist an sich klar.

Zu III. Einer der *Nichtquadratreste* zu $p=13$ ist $\varrho=8$ (§. 45. 13.), und die Producte 1.8; 2.4; 3.7; 5.12; 6.10; 9.11 sind sämmtlich $=\mathfrak{G}p+8$.

Keiner der Factoren in diesen $\frac{1}{2}(p-1)=6$ Producten ist dem andern ***gleich***; keiner kommt mehr als einmal vor, und die Factoren durchlaufen alle die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 und $12=p-1$ (5.); gemäfs (III.).

Beweis von I. ***A.*** Wenn man irgend ein z_1 aus den z (1.) mit allen den Zahlen 1, 2, 3, 4, ... $p-1$ multiplicirt und die Producte durch p dividirt, so durchlaufen die ***Reste*** nach (§. 34. I.) ***alle*** die Zahlen 1, 2, 3, 4, ... $p-1$, indem ***jedes*** z (1.) zu p ***theilerfremd*** ist. Also mufs auch irgend ein z_2 aus den Zahlen 1, 2, 3, 4, ... $p-1$

$$7. \quad z_1 z_2 = \mathfrak{G}p+1$$

geben. Und dies für ***jedes*** $z_1 = 2, 3, 4, \ldots p-2$ (1.).

B. Das z_2 zu einem ***bestimmten*** z_1 kann aber nicht ***gleich*** z_1 sein; denn sonst wären $z_1^2=\mathfrak{G}p+1$ oder $z_1^2-1=\mathfrak{G}p$ oder

$$8. \quad (z_1-1)(z_1+1) = \mathfrak{G}p$$

und es müfste entweder z_1-1 oder z_1+1 mit p aufgehen; was nicht der Fall ist, da $z_1-1<p$, und auch, da z_1 nicht gröfser als $p-2$ sein soll (1.) $z_1+1<p$ ist.

C. Ferner kann z_2 weder 1 noch $p-1$ sein; denn $z_1.1$ giebt z_1 und $z_1(p-1)$ giebt $\mathfrak{G}p-1$, also beides nicht $\mathfrak{G}p+1$; wie es sein soll. Also kann z_2 nur eine der Zahlen (1.) sein.

D. Auch kann ***nur ein*** z aus (1.), für ein ***bestimmtes*** z_1, $z_1 z_2 = \mathfrak{G}p+1$ geben; dann gäbe noch ein anderes z, z. B. z_3, $z_1 z_3=\mathfrak{G}p+1$, so wäre

$$9. \quad z_1(z_2-z_3) = \mathfrak{G}p$$

und es müfste also entweder z_1 oder z_2-z_3 mit p ***aufgehen;*** was nicht sein kann, da z_1 und z_2-z_3 beide $<p$ sind.

E. Wegen (***D.***) gehört nun zu jedem ***andern*** z_1 auch ein ***anderes*** z_2, denn sonst gehörten zu demselben z_2 zwei verschiedene z_1; was nach (***D.***) nicht sein kann; und folglich kann weder ***dasselbe*** z_1, noch ***dasselbe*** z_2, mehr als einmal vorkommen, so lange man nemlich für z_1 Zahlen nimmt, die nicht schon z_2 berührten.

Geschieht ***dieses***, so ist das zugehörige z_2 wieder das z_1, welches $z_1 z_2=\mathfrak{G}p+1$ gab; so dafs also, wenn man z_1 ***alle*** die Zahlen (1.) durchlaufen läfst, jedes Product ***zweimal*** vorkommt und folglich die ***Anzahl*** der Producte $\frac{1}{2}(p-3)$ ist, da $p-3$ Zahlen z in (1.) vorhanden sind. In diesen $\frac{1}{2}(p-3)$ Producten kommt aber dann kein z aus (1.) zweimal vor, während zugleich die z (1.) ***alle*** vorkommen.

Dieses zusammen ist was (I.) behauptet.

Von II. *F.* Was (II.) behauptet ist an sich klar.

Von III. *G* Wenn man irgend ein z_1 aus den z (5.) mit allen den Zahlen 1, 2, 3, 4, ... $p-1$ multiplicirt und die Producte durch p dividirt, so durchlaufen wieder die *Reste* nach (§. 34. I.) *alle* die Zahlen 1, 2, 3, 4, ... $p-1$, indem jedes z (5.) zu p *theilerfremd* ist. Also berühren die Reste auch *alle Nichtquadratreste* ϱ zu p, und folglich mufs irgend ein z_2 aus den Zahlen 1, 2, 3, 4, ... $p-1$ auch

$$10. \quad z_1 z_2 = \mathfrak{G}p + \varrho$$

geben, wo ϱ ein *bestimmter Nichtquadratrest* ist.

H. Dieses z_2 kann nicht *gleich* z_1 sein; denn sonst wäre

$$11. \quad z_1^2 = \mathfrak{G}p + \varrho,$$

und ϱ wäre ein *Quadratrest*, nicht ein *Nichtquadratrest.*

I. Ferner kann *nicht mehr als ein* z aus (5.) für ein bestimmtes z_1, $z_1 z_2 = \mathfrak{G}p + \varrho$ geben; denn gäbe noch ein anderes z, z. B. z_3, $z_1 z_3 = \mathfrak{G}p + \varrho$, so wäre

$$12. \quad z_1(z_2 - z_3) = \mathfrak{G}p,$$

was, wie in (*D.*), nicht sein kann.

K. Wegen (*I.*) gehört wieder zu jedem *andern* z_1 auch ein *anderes* z_2; denn sonst würden zu demselben z_2 zwei verschiedene z_1 gehören; was nach (*I.*) nicht sein kann. Folglich kann weder *dasselbe* z_1 noch *dasselbe* z_2 mehr als einmal vorkommen, so lange man für z_1 Zahlen nimmt, die nicht schon z_2 berührten.

Geschieht *dies*, so ist das zugehörige z_2 wieder das z_1, welches $z_1 z_2 = \mathfrak{G}p + \varrho$ gab; so dafs also, wenn man z_1 *alle* die Zahlen (5.) durchlaufen läfst, jedes Product *zweimal* vorkommt und folglich die *Anzahl* der Producte $\frac{1}{2}(p-1)$ ist; indem hier in (5.) $p-1$ Zahlen z vorhanden sind. In diesen $\frac{1}{2}(p-1)$ Producten kommt aber dann kein z aus (5.) zweimal vor, während zugleich die z (5.) *alle* vorkommen.

Dieses zusammen ist was (III.) behauptet.

L. Anm. Der gegenwärtige Lehrsatz beruht im wesentlichen auf den Satz (§. 34.).

§. 48.

Lehrsatz.

Für jede ungerade Stammzahl p > 1 ***ist das Product***

$$1. \quad 1.2.3.4....(p-1) = \mathfrak{G}p - 1.$$

Dieser Satz heifst nach seinem Erfinder der Wilsonsche Lehrsatz.

Beispiel.

$$2\ \begin{cases} \text{Für } p = 3 \text{ giebt (1.) } 1.2 = 2 = 1.3 - 1; \\ - \ p = 5 \ - - - \ 1.2.3.4 = 24 = 5.5 - 1; \\ - \ p = 7 \ - - - \ 1.2.3.4.5.6 = 720 = 103.7 - 1; \\ - \ p = 11 \ - - - \ 1.2.3.4.5.6.7.8.9.10 = 3628800 \\ \qquad\qquad = 329891.11; \end{cases}$$

und so weiter; dem Lehrsatze gemäfs.

Beweis *A*. Aus den Zahlen

$$3.\quad z = 2, 3, 4, \ldots . p - 2$$

geben *je zwei*, z_1 und z_2, gemäfs (§. 47. I.)

$$4.\quad z_1 z_2 = \mathfrak{G}p + 1$$

und es sind nach (§. 47. I.) $\frac{1}{2}(p-3)$ solcher Producte vorhanden, in welchen dann z_1 und z_2 *alle* die Zahlen (3.) durchlaufen, ohne dafs irgend eine mehr als einmal vorkäme.

B. Daraus folgt, dafs das Product aller dieser $\frac{1}{2}(p-3)$ Producte (4.) das Product *aller* der Zahlen (3.) ist; und da nun *jedes* derselben $= \mathfrak{G}p + 1$ ist, so ist

$$5.\quad 2.3.4.5 \ldots . (p-2) = \mathfrak{G}p + 1.$$

C. Multiplicirt man (5.) noch mit

$$6.\quad 1.(p-1) = \mathfrak{G}p - 1,$$

so ergiebt sich

$$7.\quad 1.2.3.4 \ldots . (p-1) = \mathfrak{G}p - 1;$$

welches der Lehrsatz ist.

Weiter unten werden sich noch andere Beweise dieses Satzes finden.

§. 49.

Lehrsatz.

I. *Es sei* p *eine Stammzahl* > 2, *und* r *bezeichne die positiven oder negativen* ***Quadratreste***, ϱ *die positiven oder negativen* ***Nichtquadratreste*** *zu* p, *so ist*

$$1.\quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1 \quad \text{und}$$

$$2.\quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1,$$

für ***alle*** r *und* ϱ, *und* (1.) ***nur*** *für die* r, (2.) ***nur*** *für die* ϱ. ***Alle möglichen***, *nicht mit* p *aufgehenden Zahlen* r *also, für welche die Gleichung* (1.) *Statt findet, sind* ***Quadratreste*** *zu der Stammzahl* p; *alle möglichen, nicht mit* p *aufgehenden Zahlen* ϱ, *für welche die Gleichung* (2.)

Statt findet, sind Nichtquadratreste zu der Stammzahl p. *Die Anzahl der Quadratreste* r, *so wie der Nichtquadratreste* $\varrho > 0$ *und* $< p$ *ist* $\frac{1}{2}(p-1)$.

II. *Es seien* p *und* q *zwei Stammzahlen von der Form* $4n+1$ *oder* $4n-1$, *so ist,*

3. *wenn* p *zu* q, *zugleich* q *zu* p *positiver Quadratrest oder positiver Nichtquadratrest in allen Fällen wo* p *und* q *nicht beide von der Form* $4n-1$ *sind.*

4. *Ist* p *zu* q *positiver Quadratrest, so ist zugleich* q *zu* p *positiver Nichtquadratrest, und umgekehrt, in allen Fällen, wo* p *und* q *beide von der Form* $4n-1$ *sind.*

Dieses ist das Reciprocitätsgesetz in Beziehung auf Quadratreste und Nichtquadratreste.

Beispiele zu (I.). *a.* Es sei aus (§. 45. 13.)

$$5. \quad p=13, \quad r=3 \quad \text{und} \quad \varrho=7,$$

so ist $3^{\frac{1}{2}(p-1)}=3^6=27^2=(\mathfrak{G}p+1)^2=\mathfrak{G}p+1$, gemäfs (1.); und $7^6=49^3=(\mathfrak{G}p+10)^3=\mathfrak{G}p+1000=\mathfrak{G}p-1$; gemäfs (2.).

b. Es sei aus (§. 45. 13.)

$$6. \quad p=23, \quad r=12 \quad \text{und} \quad \varrho=10,$$

so ist für (1.) $r^2=144=\mathfrak{G}p+6$, $r^4=\mathfrak{G}p+36=\mathfrak{G}p+13$, $r^8=\mathfrak{G}p+169=\mathfrak{G}p+8$, $r^{10}=(\mathfrak{G}p+8)(\mathfrak{G}p+6)=\mathfrak{G}p+2$, $r^{11}=r^{\frac{1}{2}(p-1)}=(\mathfrak{G}p+2)12=\mathfrak{G}p+1$; gemäfs (1.).

Für (2.) ist $\varrho^2=100=\mathfrak{G}p+8$, $\varrho^4=\mathfrak{G}p-5$, $\varrho^8=\mathfrak{G}p+2$, $\varrho^{10}=(\mathfrak{G}p+2)(\mathfrak{G}p+8)=\mathfrak{G}p+16$, $\varrho^{11}=(\mathfrak{G}p+16).10=\mathfrak{G}p-1$; wie gehörig.

Beispiele zu (II.) *c.* Die Stammzahlen $p=13$ und $q=29$ sind beide von der Form $4n+1$. Einer der *Quadratreste* von p ist (§. 45. 13.) $2p+3=29=q$; also ist q *Quadratrest* zu p, und $p=13$ selbst ist Quadratrest zu $q=29$; gemäfs (3.).

d. $p=5$ und $q=13$ sind beide von der Form $4n+1$. Einer der *Nichtquadratreste* zu 5 ist (§. 45. 13.) $2.5+3=13$, also $=q$, und zugleich ist $p=5$ selbst *Nichtquadratrest* zu $q=13$; gemäfs (3.).

e. $p=23$, von der Form $4n-1$, ist *Quadratrest* zu $q=29=4n+1$ (§. 45. 13.); auch $q=29$ ist *Quadratrest* zu $p=23$, nemlich $=1.p+6$; gemäfs (3.).

f. $p = 11$, von der Form $4n-1$, ist *Nichtquadratrest* zu $q = 29$ (§. 45. 13.); und auch $q = 29$ ist *Nichtquadratrest* zu $p = 11$, nemlich $= 2p + 7$; gemäfs (3.).

g. $p = 13$, von der Form $4n+1$, ist *Quadratrest* zu $q = 23 = 4n-1$; und auch $q = 23$ ist *Quadratrest* zu $p = 13$ (§. 45. 13.), nemlich $= 1.p + 4$; gemäfs (3.).

h. $p = 17 = 4n+1$ ist *Nichtquadratrest* zu $q = 31 = 4n-1$; und auch $q = 31$ ist *Nichtquadratrest* zu $p = 17$, nemlich $= 1.p + 14$ (§. 45. 13.), gemäfs (3.).

i. $p = 7 = 4n-1$ ist *Quadratrest* zu $q = 31 = 4n-1$. Dagegen ist $q = 31$ *Nichtquadratrest* zu $p = 7$, nemlich $= 4.p + 3$ (§. 45. 13.); gemäfs (4.).

k. $p = 11 = 4n-1$ ist *Nichtquadratrest* zu $q = 31 = 4n-1$. Dagegen ist $q = 31$ *Quadratrest* zu $p = 11$, nemlich $= 2p + 9$ (§. 45. 13.); gemäfs (4.).

Erster Beweis von (I.). *A.* Nach dem Fermatschen Lehrsatze (40.) ist

$$7. \quad z^{p-1} - 1 = \mathfrak{G}p,$$

und daraus folgt, weil $p-1$ *immer gerade* ist,

$$8. \quad (z^{\frac{1}{2}(p-1)} - 1)(z^{\frac{1}{2}(p-1)} + 1) = \mathfrak{G}p,$$

also mufs entweder $z^{\frac{1}{2}(p-1)} - 1$ oder $z^{\frac{1}{2}(p-1)} + 1$ mit p *aufgehen*, das heifst es mufs

$$9. \quad \text{entweder } z^{\frac{1}{2}(p-1)} - 1 = \mathfrak{G}p$$

$$10. \quad \text{oder } z^{\frac{1}{2}(p-1)} + 1 = \mathfrak{G}p$$

sein.

B. Die Gleichung (7.) hat $p-1$ *Wurzeln*, denn sie findet nach (§. 40.) für *alle* die $p-1$ Werthe $1, 2, 3, 4, \ldots p-1$ von z Statt. Also mufs auch (8.), und folglich müssen (9. und 10.), diese letztern *zusammen*, für $p-1$ verschiedene Werthe von z Statt finden.

C. Ein- und derselbe Werth von z kann nicht (9.) und (10.) *zugleich* erfüllen, denn sonst wäre, (9.) von (10.) abgezogen,

$$11. \quad z^{\frac{1}{2}(p-1)} + 1 - (z^{\frac{1}{2}(p-1)} - 1) = 2 = \mathfrak{G}p,$$

und 2 geht *nicht* mit p auf. Alle Wurzeln von (9.) müssen also von denen von (10.) *verschieden* sein.

D. Nun kann nach (§. 44.) (9.), und eben so (10.), *nicht mehr* als $\frac{1}{2}(p-1)$ Wurzeln haben. Deshalb kann z. B. (9.) auch *nicht weniger* als $\frac{1}{2}(p-1)$ Wurzeln haben, denn wäre das, so müfste, weil (9. und 10.) *zusammen* $p-1$ Wurzeln haben müssen (*B.*), (10.) *mehr* als $\frac{1}{2}(p-1)$ Wurzeln

haben, was nach (§. 44.) nicht sein kann. Folglich mufs (9.), da es ***nicht mehr*** und ***nicht weniger*** als $\frac{1}{2}(p-1)$ Wurzeln haben kann, nothwendig gerade $\frac{1}{2}(p-1)$ verschiedene Wurzeln haben, und folglich (10.) die übrigen $\frac{1}{2}(p-1)$ Wurzeln, die nach (*C.*) alle von den Wurzeln von (9.) verschieden sind. Die Gleichungen (9. und 10.) theilen sich also zu zwei ***gleichen*** Theilen in die $p-1$ Wurzeln $1, 2, 3, 4, \ldots\ldots p-1$ von (7.).

E. Setzt man nun für alle Werthe von z,

$$12. \quad z^2 = \mathfrak{G}p + r,$$

wo $r > 0$ und $< p$, so bezeichnet r alle ***Quadratreste.*** Nimmt man von (12.) die $\frac{1}{2}(p-1)$ten Potenz, so ergiebt sich

$$13. \quad z^{2\cdot\frac{1}{2}(p-1)} = z^{p-1} = (\mathfrak{G}p + r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + r^{\frac{1}{2}(p-1)} \text{ (§. 11. 20.)},$$

und da nach dem Fermatschen Lehrsatz (§. 40.), für *alle* Werthe von z, $z^{p-1} = \mathfrak{G}p + 1$ ist,

$$\mathfrak{G}p + 1 = \mathfrak{G}p + r^{\frac{1}{2}(p-1)} \text{ oder}$$

$$14. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1 \quad \text{oder} \quad r^{\frac{1}{2}(p-1)} - 1 = \mathfrak{G}p.$$

F. Es sind aber die Quadratreste r, da sie > 0 und $< p$ sind, ebensowohl Werthe von z: also ist (14.) nichts anders als (9.); und da nun (9.) zufolge (*D.*) nothwendig für $\frac{1}{2}(p-1)$ Werthe von z (für nicht mehr und nicht weniger) Statt findet, so hat in (14.) r nothwendig $\frac{1}{2}(p-1)$ verschiedene Werthe. Folglich giebt es nothwendig $\frac{1}{2}(p-1)$ verschiedene ***Quadratreste*** r, nicht mehr und nicht weniger, unter den Werthen von $z > 0$ und $< p$, und für jeden derselben findet die Gleichung (14.) Statt, welche diejenige (1.) des Lehrsatzes ist.

G. Da r in (14.) oder (1.) ***nur*** $\frac{1}{2}(p-1)$ Werthe haben kann, so bleiben $\frac{1}{2}(p-1)$ Werthe von z übrig, welche nach (*C.*) diejenigen sind, die der Gleichung (10.) genugthun. Da sie keine Quadratreste sind, für welche ***nur*** die Gleichung (9.) gilt, so sind sie die *Nichtquadratreste* ϱ, und folglich giebt es auch $\frac{1}{2}(p-1)$ *Nichtquadratreste*, und für jeden derselben findet nach (10.) die Gleichung

$$15. \quad \varrho^{\frac{1}{2}(p-1)} + 1 = \mathfrak{G}p$$

Statt, welche nichts anderes als die Gleichung (2.) des Lehrsatzes ist.

H. Übrigens kann r und ϱ auch $> p$ sein, z. B. r_1 und ϱ_1, wenn nur

$$16. \quad r_1 = \mathfrak{G}p + r \quad \text{und}$$

$$17. \quad \varrho_1 = \mathfrak{G}p + \varrho$$

ist. Dieses zusammen behauptet (I.).

Zweiter Beweis von I. *I.* Aus den Zahlen

$$18.\quad z = 1, 2, 3, 4, \dots p-1$$

geben je *zwei*, z_1 und z_2, gemäfs (§. 47. III.),

$$19.\quad z_1 z_2 = \mathfrak{G}p + \varrho,$$

wo ϱ ein beliebiger *Nichtquadratrest* zu p ist, und es sind nach (§. 47. III.) $\frac{1}{2}(p-1)$ solcher Producte vorhanden, in welchen dann z_1 und z_2 *alle* die Zahlen (13.) durchlaufen, ohne dafs irgend eine mehr als einmal vorkäme.

K. Daraus folgt, dafs das Product aller der $\frac{1}{2}(p-1)$ Producte (19.) das Product *aller* der Zahlen (18.) ist; und da nun *jedes* der $\frac{1}{2}(p-1)$ Producte (19.) $z_1 z_2 = \mathfrak{G}p + \varrho$ giebt, so ist

$$20.\quad 1.2.3.4 \dots (p-1) = (\mathfrak{G}p + \varrho)^{\frac{1}{2}(p-1)} = \mathfrak{G}p + \varrho^{\frac{1}{2}(p-1)}.$$

L. Aber gemäfs (§. 48.) ist

$$21.\quad 1.2.3.4 \dots (p-1) = \mathfrak{G}p - 1,$$

also ist, zufolge (20. und 21.), $\mathfrak{G}p + \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1$ oder

$$22.\quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1:$$

gemäfs (2.).

M. Für *jede* Zahl $< p$, also auch für jeden *Quadratrest* r zu p, ist nach dem Fermatschen Satz (§. 40.)

$$23.\quad r^{p-1} = \mathfrak{G}p + 1.$$

Daraus folgt

$$24.\quad r^{p-1} - 1 \quad \text{oder} \quad (r^{\frac{1}{2}(p-1)} + 1)(r^{\frac{1}{2}(p-1)} - 1) = \mathfrak{G}p,$$

also mufs entweder $r^{\frac{1}{2}(p-1)} + 1$ oder $r^{\frac{1}{2}(p-1)} - 1$ mit p *aufgehen,* das heifst, es mufs

$$25.\quad \text{entweder } r^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1,$$

$$26.\quad \text{oder } r^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1$$

sein. Das erste kann nicht sein, denn sonst müfste nach (22.) r nicht ein Quadratrest, sondern ein *Nichtquadratrest* ϱ sein. Also kann nur

$$27.\quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1$$

sein; gemäfs (1.).

Beweis von (II.). *N.* Nach dem Reciprocitätsgesetze (§. 42.) ist *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1$, oder *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1$, wenn p und q *nicht beide* von der Form $4n-1$ sind. Also ist in diesem Fall, gemäfs (1. und 2.), entweder q einer der *Quadratreste* zu p und *zugleich* p einer der *Quadratreste* zu q, oder q einer der *Nichtquadratreste* zu p und *zugleich* p einer der *Nichtquadratreste* zu q; gemäfs (3.).

O. Sodann ist nach dem Reciprocitätsgesetze (§. 42.) *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1$, oder *zugleich* $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$ und $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1$, wenn p und q *beide* von der Form $4n-1$ sind. Also ist in diesem Falle gemäfs (1. und 2.) entweder q einer der *Quadratreste* zu p, und *zugleich* p einer der *Nichtquadratreste* zu q, oder q einer der Nichtquadratreste zu p, und *zugleich* p einer der *Quadratreste* zu q, gemäfs (4.).

Erste Anm. *P.* Der *erste* Beweis von (I.), welcher (II.) unmittelbar begründet, beruht insbesondere auf dem Fermatschen Satze (§. 40.) und auf dem Satze (§. 44.) von der Anzahl der Wurzeln von Zahlengleichungen; der *zweite* Beweis von (I.) beruht auf dem Wilsonschen Satze (§. 48.) und auf dem Satze (§. 47.) von den *zusammengehörigen* Zahlen. Der zweite Beweis bedarf also weniger Vordersätze als der erste. Eigenthümlich ist in dem ersten Beweise die Folgerung in (*D.*), dafs, da von den *beiden* Gleichungen (9. und 10.) keine *mehr als* $\frac{1}{2}(p-1)$ Wurzeln haben kann und beide zusammen nothwendig $p-1$ Wurzeln haben, jede $\frac{1}{2}(p-1)$ Wurzeln haben *mufs*.

Zweite Anm. *Q.* Wegen der Beziehung (II.) des Reciprocitäts- oder Gegenseitigkeits-Gesetzes auf die *Quadratreste* und *Nichtquadratreste* könnte man dasselbe *Gegenquadratrestgesetz* nennen. Diese Benennung würde *deutlicher bezeichnen* was gemeint ist, als das Wort *Gegenseitigkeitsgesetz.* Da es indessen etwas länger ist und das Gegenseitigkeitsgesetz auch in seiner ursprünglichen Form (§. 42.) vorkommt, so wollen wir von „*Gegenquadratrestgesetz*" nicht Gebrauch machen.

Ferner wäre *Gegenheitsgesetz* kürzer und einfacher als Gegenseitigkeitsgesetz, und *Gegenheit* würde nach dem Vorbilde von *Gleichheit, Allgemeinheit, Besonderheit, Gewifsheit* u. s. w. grammatisch nicht unrichtig sein. Da indessen wieder das Wort Gegenheit noch vielleicht *zu neu* ist, so wollen wir die kürzere Benennung blofs anheimstellen, und uns nur begnügen, das verstümmelte fremde Wort Reciprocität zu vermeiden, mithin den Satz (§. 42.) oder (§. 49. II.) *Gegenseitigkeitsgesetz* nennen.

§. 50.

Lehrsatz.

I. *Für alle Stammzahlen* $p = 4n+1$ *sind die zeichenfreien Werthe der positiven und der negativen echten Quadratreste dieselben. Gleiches gilt von den Nichtquadratresten.*

II. *Für alle Stammzahlen* $p = 4n - 1$ *sind die positiven echten Quadratreste die zeichenfreien Werthe der negativen echten Nichtquadratreste, und die positiven echten Nichtquadratreste die zeichenfreien Werthe der negativen echten Quadratreste.*

Beispiele. Was (I.) behauptet, zeigt sich in (§. 45. 13.) an den Stammzahlen 5, 13, 17 und 29, die von der Form $4n+1$ sind.

Was (II.) behauptet, zeigt sich in (§. 45. 13.) an den Stammzahlen 3, 7, 11, 19, 23 und 31, die von der Form $4n-1$ sind.

Beweis *A*. Für *alle*, und folglich auch für alle *echten positiven Quadratreste* r findet nach (§. 49. 1.) die Gleichung

$$1. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1,$$

und für *alle*, also auch für alle echten positiven *Nichtquadratreste* nach (§. 49. 2.), die Gleichung

$$2. \quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$$

Statt.

B. Alle echten *negativen* Quadratreste werden durch $r-p$ ausgedrückt, also ihre *zeichenfreien* Werthe durch $p-r$; denn $p-r$ ist >0 und $<p$.

Je nachdem also die durch $p-r$ ausgedrückten Zahlen

$$3. \quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1, \text{ oder}$$

$$4. \quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$$

geben, werden sie zufolge (§. 49. 1. u. 2.) *Quadratreste* oder *Nichtquadratreste* zu p sein.

C. Da

$$5. \quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+(-r)^{\frac{1}{2}(p-1)}$$

ist, so erfordert nach (3.) das Erste, dafs

$$6. \quad \mathfrak{G}p+(-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1, \quad \text{also} \quad (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1,$$

das Andere nach (4.), dafs

$$7. \quad \mathfrak{G}p+(-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1, \quad \text{also} \quad (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$$

sei.

D. Ist nun $p=4n+1$, so ist $\frac{1}{2}(p-1)=2n$ und folglich $\frac{1}{2}(p-1)$ eine *gerade* Zahl. Also ist alsdann $(-r)^{\frac{1}{2}(p-1)}=(+r)^{\frac{1}{2}(p-1)}$, und da nach (1.) $(+r)^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$ ist, so wird für $p=4n+1$ die Gleichung (6.) erfüllt. Also sind für $p=4n+1$ die Zahlen $p-r$ echte positive *Quadratreste*, und folglich sind die echten *negativen* Quadratreste $r-p$ ihrem *zeichenfreien* Werthe nach den echten positiven *Quadratresten* r *gleich.*

Und da die echten positiven *Nichtquadratreste* ϱ übrig bleiben, wenn man die echten positiven *Quadratreste* r aus den Zahlen $1, 2, 3, 4, \ldots. p-1$ wegnimmt; desgleichen die echten negativen *Nichtquadratreste* $-\varrho$, wenn man die echten negativen *Quadratreste* aus $-(1, 2, 3, 4, \ldots. p-1)$ wegläfst, so sind auch nothwendig die echten ***negativen Nichtquadratreste*** ihrem ***zeichenfreien*** Werthe nach den echten ***positiven Nichtquadratresten gleich.***

Dieses ist was (I.) behauptet.

E. Ist dagegen $p=4n-1$, so ist $\frac{1}{2}(p-1)=2n-1$, und folglich $\frac{1}{2}(p-1)$ eine *ungerade* Zahl. Also ist alsdann $(-r)^{\frac{1}{2}(p-1)}=-(+r)^{\frac{1}{2}(p-1)}$, und da nach (1.) $(+r)^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$, also $-(+r)^{\frac{1}{2}(p-1)}=-\mathfrak{G}p-1=\mathfrak{G}p-1$ ist, so wird für $p=4n-1$ die Gleichung (7.) erfüllt. Also sind für $p=4n-1$ die Zahlen $p-r$ echte positive *Nichtquadratreste,* und folglich die echten ***negativen*** Quadratreste $r-p$ ihrem ***zeichenfreien*** Werthe $p-r$ nach den echten ***positiven Nichtquadratresten*** ϱ gleich.

Und da nun die echten negativen *Nichtquadratreste* $-\varrho$ durch $\varrho-p$ ausgedrückt werden, so sind sie, weil $p-r=\varrho$ war, gleich $p-r-p=-r;$ folglich ist der ***zeichenfreie*** Werth r der ***negativen*** echten ***Quadratreste*** $-r$ der der ***negativen*** echten *Nichtquadratreste* ϱ.

Dieses ist was (II.) behauptet.

F. Anm. Der Satz beruht insbesondere auf (§. 49.)

§. 51.

Lehrsatz.

I. ***Für jede Stammzahl*** p $=4n+1$ ***ist die Summe der zeichenfreien Werthe je zweier positiver oder je zweier negativer echter Quadratreste, so wie die Summe der zeichenfreien Werthe je zweier positiver oder je zweier negativer echter Nichtquadratreste, gleich*** p.

II. ***Für jede Stammzahl*** p $=4$n-1 ***ist die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten Quadratrests, so wie die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten Nichtquadratrests gleich*** p.

Beispiel. In (§. 45. 13.) sieht man was (I.) behauptet an den Stammzahlen $p=5, 13, 17$ **und** 29**, die von der Form** $4n+1$ **sind, und was (II.) behauptet an den Stammzahlen** $3, 7, 11, 19$ 23 **und** 31**, die von der Form** $4n-1$ **sind.**

Beweis *A.* Je nachdem $p-r$ ein echter positiver *Quadratrest,* oder ein echter positiver *Nichtquadratrest* ist, wird die Summe zweier echter positiver, oder die Summe eines echten positiven und eines echten negativen *Nichtquadratrests* gleich p sein.

B. Soll nun $p-r$ ein echter positiver *Quadratrest* sein, so mufs es nach (§. 49. 1.) die Gleichung

$$1.\quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$$

erfüllen. Soll $p-r$ ein echter positiver *Nichtquadratrest* sein, so mufs es nach (§. 49. 2.) der Gleichung

$$2.\quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$$

genugthun.

C. Ersteres geschieht, wenn $p=4n+1$ ist; denn die Gleichung (1.) ist so viel als $\mathfrak{G}p+(-r)^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$ oder

$$3.\quad (-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1,$$

und da hier $\frac{1}{2}(p-1)=2n=$ einer *geraden* Zahl ist, so ist $(-r)^{\frac{1}{2}(p-1)}=(+r)^{\frac{1}{2}(p-1)}$, also in (3.)

$$4.\quad +r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1,$$

und folglich auch nach (1.)

$$5.\quad (p-r)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1.$$

Mithin ist $p-r$ wirklich ein echter positiver *Quadratrest.* Also ist zunächst

a. Die *Summe* je zweier echter positiver Quadratreste $=p$.

b. Die *zeichenfreien* Werthe der echten negativen *Quadratreste* sind in dem Falle $p=4n+1$ nach (§. 50. I.) den echten positiven *Quadratresten gleich.* Also ist auch die Summe der *zeichenfreien* Werthe zweier echter negativer Quadratreste $=p$.

c. Die positiven echten *Nichtquadratreste* ϱ bleiben aus den Zahlen $1, 2, 3, 4, \ldots\ldots p-1$ übrig, wenn man davon die echten positiven Quadratreste r wegläfst. Also ist *kein* ϱ einem r gleich. Mithin ist auch kein $p-\varrho$ einem $p-r$ gleich, und mithin, da nach (*a.*) *jedes* $p-r$ einem r gleich ist, auch kein $p-\varrho$ einem r. Aber $p-\varrho$ ist, eben wie ϱ, nothwendig unter den Zahlen $1, 2, 3, 4, \ldots\ldots p-1$ anzutreffen, weil $p-\varrho>0$ und $<p$ ist: also ist nothwendig jedes $p-\varrho$ einem ϱ *gleich.* Das heifst: auch die Summe je zweier echter positiver *Nichtquadratreste* ist $=p$.

d. Endlich sind nach (§. 50. 1.) die zeichenfreien Werthe der negativen echten *Nichtquadratreste* den positiven echten *Nichtquadratresten gleich.*

Also ist auch die Summe der zeichenfreien Werthe je zweier echter negativer *Nichtquadratreste* $= p$.

Dieses zusammen ist, was (I.) behauptet.

D. Die zweite Gleichung (2.) in (*B.*) wird erfüllt, wenn $p = 4n - 1$ ist; denn die Gleichung (2.) ist so viel als $\mathfrak{S}p + (-r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1$ oder

$$6. \quad (-r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1,$$

und da hier $\frac{1}{2}(p-1) = 2n - 1 =$ einer *ungeraden* Zahl ist, so ist $(-r)^{\frac{1}{2}(p-1)} = -(+r)^{\frac{1}{2}(p-1)}$, also ist in (6.)

$$7. \quad -(+r)^{\frac{1}{2}(p-1)} = \mathfrak{S}p - 1 \text{ oder}$$

$$8. \quad (+r)^{\frac{1}{2}(p-1)} = -\mathfrak{S}p + 1 = \mathfrak{S}p + 1.$$

Dieses ist der Gleichung (§. 49. 1.) für alle echten positiven *Quadratreste* $+r$ gemäfs. Also erfüllt in dem gegenwärtigen Falle $p = 4n - 1$, $p - r$ die Gleichung (2.) wirklich, und folglich ist für $p = 4n - 1$ die Summe der zeichenfreien Werthe je eines positiven Quadratrests und eines positiven echten *Nichtquadratrests* $= p$.

Aber die positiven echten *Nichtquadratreste* sind nach (§. 50. II.) den zeichenfreien Werthen der negativen echten *Quadratreste gleich.* Also ist

a. Die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten *Quadratrestes* $= p$.

d. Ferner sind nach (§. 50. II.) die echten positiven *Quadratreste* den zeichenfreien Werthen nach den negativen echten *Nichtquadratresten* gleich. Also ist auch die Summe der zeichenfreien Werthe je eines positiven und eines negativen echten *Nichtquadratrestes* $= p$.

Dieses zusammen ist was (II.) behauptet.

Anm. *E.* Der Beweis beruht auf (§. 49. und 50.). Eigenthümlich ist der Schlufs in (*C. c.*).

§. 52.

Lehrsatz.

I. ***Das Product einer beliebigen Anzahl von Quadratresten zu einer und derselben Stammzahl* p *ist ein Quadratrest zu* p.**

II. ***Das Product einer beliebigen geraden Anzahl von Nichtquadratresten, eben so, ist ein Quadratrest.***

III. ***Das Product einer beliebigen ungeraden Anzahl von beliebigen Nichtquadratresten, eben so, ist ein Nichtquadratrest.***

IV. ***Das Product eines Quadratrestes und eines Nichtquadratrestes ist ein Nichtquadratrest.***

Beispiele. 1. Zu I. $+8$, -10 und 4 sind *Quadratreste* zu $p=7$ (§. 45. 13.), und ihr Product ist $-320 = -46.7+2$, also ebenfalls ein *Quadratrest* zu p.

2. Zu II. 18, -5, 7 und 15 sind *Nichtquadratreste* zu $p=13$ (§. 45. 13.), und ihr Product ist $-9450 = -727.13+1$, also ein *Quadratrest* zu p.

3. Zu III. -32, -32 und 40 sind *Nichtquadratreste* zu $p=29$ (§. 45. 13.), und ihr Product $32^2.40$ ist $=40960 = 1412.29+12$, also ebenfalls ein *Nichtquadratrest* zu p.

4. Zu IV. -11 ist ein *Quadratrest* und $+33$ ein *Nichtquadratrest* zu $p=23$ (§. 45. 13.), und ihr Product -363 ist $= -16.23+5$, also ein *Nichtquadratrest* zu p.

Beweis. Für jeden *beliebigen Quadratrest* r ist nach (§. 49. 1.)

$$1. \quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$$

und für jeden *beliebigen Nichtquadratrest* ϱ nach (§. 49. 2.)

$$2. \quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1.$$

Multiplicirt man also eine *beliebige Anzahl* von r in einander, so ist das Product gemäfs (1.) immer $=\mathfrak{G}p+1$, und folglich ebenfalls ein *Quadratrest;* gemäfs (I.).

Multiplicirt man eine *beliebige gerade Anzahl* von *Nichtquadratresten* in einander, so ist das Product gemäfs (2.) immer $=\mathfrak{G}p+1$, also ebenfalls ein *Quadratrest;* gemäfs (II.).

Multiplicirt man dagegen eine *beliebige ungerade* Anzahl von *Nichtquadratresten* in einander, so ist das Product gemäfs (2.) immer $=\mathfrak{G}p-1$, und folglich ein *Nichtquadratrest;* gemäfs (III.).

Multiplicirt man (1.) in (2.), so ist das Product $=\mathfrak{G}p-1$, und folglich ein *Nichtquadratrest;* gemäfs (IV.).

Anm. Der Beweis geht unmittelbar aus (§. 49.) hervor.

§. 53.

Lehrsatz.

I. $+1$ ist *Quadratrest* zu allen Stammzahlen ohne Ausnahme.

II. -1 ist *Quadratrest* zu allen Stammzahlen $p=4n+1$
und *Nichtquadratrest* zu allen Stammzahlen $p=4n-1$.

III. $+2$ ist *Quadratrest* zu allen Stammzahlen $p=8n+1$ und $p=8n-1$
und *Nichtquadratrest* zu allen Stammzahlen $p=8n+3$ und $p=8n-3$.

IV. -2 ist ***Quadratrest*** zu allen Stammzahlen $p=8n+1$ und $p=8n+3$ und ***Nichtquadratrest*** zu allen Stammzahlen $p=8n-1$ und $p=8n-3$.

Beispiele. *a.* In allen den Beispielen (§. 45. 13.) ist, wie sich zeigt, $+1$ einer der ***Quadratreste.***

b. -1 ist unter den ***Quadratresten*** zu $p=5, 13, 17$ und 29, und diese p sind von der Form $4n+1$.

-1 ist unter den ***Nichtquadratresten*** zu $p=3, 7, 11, 19, 23$ und 31, und diese Stammzahlen sind von der Form $4n-1$.

c. $+2$ ist unter den ***Quadratresten*** zu $p=17=8n+1$ und $p=7, 23$ und $31=8n-1$.

$+2$ ist unter den ***Nichtquadratresten*** zu $p=3, 11$ und $19=8n+3$ und $p=5, 13$ und $29=8n-3$.

d. -2 ist unter den ***Quadratresten*** zu $p=17=8n+1$ und $p=3, 11$ und $19=8n+3$.

-2 ist unter den ***Nichtquadratresten*** zu $p=7$ und $23=8n-1$ und $p=5, 13$ und $29=8n-3$.

Beweis von I. ***A.*** Für alle Zahlen r, welche Quadratreste zu der Stammzahl p sind, ist nach (§. 49. 1.)

$$1.\quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1.$$

Dieser Gleichung wird durch $r=+1$ genuggethan; was auch p sein mag. Also ist $+1$ ***Quadratrest*** zu ***jeder*** Stammzahl p.

Beweis von II. ***B.*** Der Gleichung (1.) wird durch $r=-1$ nur dann genuggethan, wenn $\frac{1}{2}(p-1)$ ***gerade*** ist. Dieses ist der Fall für $p=4n+1$, welches $\frac{1}{2}(p-1)=2n$ giebt; nicht für $p=4n-1$; denn dieses giebt $\frac{1}{2}(p-1)=2n-1$, also eine ***ungerade*** Zahl. Mithin ist -1 ***Quadratrest*** zu allen Stammzahlen $p=4n+1$.

C. Sodann ist für alle Zahlen ϱ, welche ***Nichtquadratreste*** zu der Stammzahl p sind, nach (§. 49. 2.),

$$2.\quad \varrho^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1.$$

Dieser Gleichung wird durch $\varrho=-1$ genuggethan, wenn $\frac{1}{2}(p-1)$ ***ungerade*** ist. Dieses ist, wie so eben in (***B.***) bemerkt, der Fall, wenn $p=4n-1$ ist. Also ist -1 ***Nichtquadratrest*** zu allen Stammzahlen $p=4n-1$.

Beweis von III. ***D.*** Man multiplicire alle die Zahlen $1, 2, 3, 4, \ldots \ldots \frac{1}{2}(p-1)$ mit 2. Dieses giebt

3. Für $p=8n+1$, 2.1, 2.2, 2.3, 2.4, ... $2.2n$ und
$2(2n+1)$, $2(2n+2)$, $2(2n+3)$, ... $2.4n$;

4. Für $p=8n-1$, 2.1, 2.2, 2.3, 2.4, ... $2(2n-1)$ und
$2.2n$, $2(2n+1)$, $2(2n+2)$, ... $2(4n-1)$;

5. Für $p=8n+3$, 2.1, 2.2, 2.3, 2.4, ... $2.2n$ und
$2(2n+1)$, $2(2n+2)$, $2(2n+3)$, ... $2(4n+1)$;

6. Für $p=8n-3$, 2.1, 2.2, 2.3, 2.4, ... $2(2n-1)$ und
$2.2n$, $2(2n+1)$, $2(2n+2)$, ... $2(4n-2)$.

In diesen vier verschiedenen Productenreihen sind alle die, welche *vor* dem Worte *und* stehen, $<\frac{1}{2}p$, denn die *gröfsten* derselben sind $2.2n=4n<\frac{1}{2}(8n+1)$, $2(2n-2)=4n-1<\frac{1}{2}(8n-1)$; $2.2n=4n<\frac{1}{2}(8n+3)$ und $2(2n-1)=4n-2<\frac{1}{2}(8n-3)$: alle Producte, die nach dem Worte *und* stehen, sind $>\frac{1}{2}p$ oder $<p$; denn die *kleinsten* derselben sind $2(2n+1)=4n+2>\frac{1}{2}(8n+1)$; $2.2n=4n>\frac{1}{2}(8n-1)$; $2(2n+1)=4n+2>\frac{1}{2}(8n+3)$ und $2.2n=4n>\frac{1}{2}(8n-3)$; die gröfsten dagegen $2.4n=8n<8n+1$; $2(4n-1)=8n-2<8n-1$; $2(4n+1)=8n+2<8n+3$ und $2(4n-2)=8n-4<8n-3$.

E. Die *Anzahl* der Producte in (3. 4. 5. 6.), die $>\frac{1}{2}p$ sind, und welche durch x bezeichnet werden mag, ist

7. In (3.), für $p=8n+1$, $x=2n$, also *gerade;*

8. In (4.), für $p=8n-1$, $x=2n$, also *gerade;*

9. In (5.), für $p=8n+3$, $x=2n+1$, also *ungerade;*

10. In (6.), für $p=8n-3$, $x=2n-1$, also *ungerade.*

F. Nun ist zufolge (§. 41. 3. und 4.), wenn man daselbst $z=2$ setzt,

11. $2^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$, wenn x *gerade* und

12. $2^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1$, wenn x *ungerade* ist.

Also erfüllt $r=2$ die Gleichung (1.), wenn x *gerade,* also $p=8n+1$ oder $p=8n-1$, und $\varrho=2$ die Gleichung (2.), wenn x *ungerade,* also $p=8n+3$ oder $p=8n-3$ ist. Und folglich ist $+2$ *Quadratrest* zu $p=8n+1$ und $p=8n-1$, und *Nichtquadratrest* zu $p=8n+3$ und $p=8n-3$; gemäfs (III.).

Erster Beweis von IV. *G.* Es war $+1$ *Quadratrest* zu *allen* Stammzahlen ohne Ausnahme, also zu $p=8n+1$, $8n-1$, $8n+3$ und $8n-3$ (I.). Ferner war -1 *Quadratrest* zu $p=4n+1$ (II.), also zu den Stammzahlen $p=8n+1$ und $p=8n-3$, die von der Form $4n+1$ sind, wie sich zeigt, wenn man in $4n+1$ erst $2n$ und dann $2n-1$ statt n

setzt (was geschehen darf, indem $2n$ und $2n-1$ zusammen ebensowohl *alle* geraden und ungeraden Zahlen ausdrücken, wie n selbst), und was dann $4.2n+1=8n+1$ und $4(2n-1)+1=8n-3$ giebt. Und endlich war -1 *Nichtquadratrest* zu $p=4n-1$ (II.), also zu den Stammzahlen $p=8n-1$ und $p=8n+3$, die von der Form $4n-1$ sind, wie sich zeigt, wenn man in $4n-1$ erst $2n$ und dann $2n+1$ statt n setzt, was wie vorhin geschehen darf und was $4.2n-1=8n-1$ und $4(2n+1)-1=8n+3$ giebt.

H. Nimmt man dies mit dem was der Lehrsatz in (III.) für $+2$ aussagt zusammen, so ergiebt sich Folgendes:

13.

Zu $p=$	$8n+1$,	$8n-1$,	$8n+3$ und	$8n-3$	
sind	$+1$	$+1$	$+1$	$+1$	*Quadratrest*
	-1	...	...	...	
	$+2$	$+2$	...	...	
und	...	-1	-1	...	*Nichtquadratrest.*
	...	...	$+2$	$+2$	

Nun erhält man in (13.) -2, wenn man

14. Für $p=8n+1$, den *Quadratrest* -1 mit dem *Quadratrest* $+2$,
- $p=8n-1$, den *Quadratrest* $+2$ mit dem *Nichtquadratrest* -1,
- $p=8n+3$, den *Nichtquadratrest* -1 mit dem *Nichtquadratrest* $+2$,
- $p=8n-3$, den *Quadratrest* -1 mit dem *Nichtquadratrest* $+2$

multiplicirt. Aber das Product zweier *Quadratreste* und zweier *Nichtquadratreste* ist nach (§. 52. I. und II.) ein *Quadratrest*, und das Product eines *Quadratrests* und eines *Nichtquadratrests* nach (§. 52. III.) ein *Nichtquadratrest:* also folgt aus (14.), dafs -2 *Quadratrest* zu $p=8n+1$ und $p=8n+3$ und *Nichtquadratrest* zu $p=8n-1$ und $p=8n-3$ ist; gemäfs (IV.).

Zweiter Beweis von IV. *I.* Man multiplicire (11. und 12.) mit $(-1)^{\frac{1}{2}(p-1)}$. Dieses giebt

15. $(-2)^{\frac{1}{2}(p-1)}=\mathfrak{G}p+(-1)^{\frac{1}{2}(p-1)}$, wenn x *gerade*, also $p=8n+1$ oder $p=8n-1$ ist (7. und 8.), und

16. $(-2)^{\frac{1}{2}(p-1)}=\mathfrak{G}p-(-1)^{\frac{1}{2}(p-1)}$, wenn x *ungerade*, also $p=8n+3$ oder $p=8n-3$ ist (9. und 10.).

Nun ist

$$17.\ \begin{cases} 1. & \text{Für } p=8n+1,\ \tfrac{1}{2}(p-1)=4n, \text{ also } \textit{gerade;} \\ 2. & \text{- } p=8n-1,\ \tfrac{1}{2}(p-1)=4n-1, \text{ also } \textit{ungerade;} \\ 3. & \text{- } p=8n+3,\ \tfrac{1}{2}(p-1)=4n+1, \text{ also } \textit{ungerade;} \\ 4. & \text{- } p=8n-3,\ \tfrac{1}{2}(p-1)=4n-2, \text{ also } \textit{gerade;} \end{cases}$$

folglich geben (15. und 16.)

$$18.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1 \quad \text{für} \quad p = 8n+1;$$
$$19.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1 \quad \text{für} \quad p = 8n-1;$$
$$20.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1 \quad \text{für} \quad p = 8n+3;$$
$$21.\quad (-2)^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1 \quad \text{für} \quad p = 8n-3.$$

Die Gleichungen (18. und 20.) erfüllen diejenigen (1.) für $r = -2$, also ist -2 *Quadratrest* zu $p = 8n+1$ und $8n+3$. Dagegen erfüllen die Gleichungen (19. und 21.) die Gleichung (2.) für $\varrho = -2$, also ist -2 *Nichtquadratrest* zu $p = 8n-1$ und $p = 8n-3$; gemäfs (IV.).

Anm. *1.* Die Beweise beruhen auf einer Verbindung der Sätze (§. 41. 49. und 52.).

§. 54.

Lehrsatz.

Wenn in den Zahlengleichungen (S. §. 43.)

$$1.\quad z^{\delta} = \mathfrak{G}p+r \quad \text{und}$$
$$2.\quad z^{\lambda} = \mathfrak{G}p+\varrho$$

p *eine Stammzahl ist,* r *und* $\varrho > 0$ *und* $<$ p *sind, und der Exponent* δ *in* $p-1$, *der Exponent* λ *in* δ *und also ebenfalls in* $p-1$ *aufgeht, so dafs z. B.*

$$3.\quad \delta\tau = p-1 \quad \textit{und}$$
$$4.\quad x\lambda = \delta$$

ist, und man setzt in (1.) *der Reihe nach*

$$5.\quad z = 1, 2, 3, 4, \ldots\ p-1,$$

so bekommt

I. *Der Rest* r *in* (1.) τ *verschiedene Werthe aus den Zahlen* (5.), *und zu jedem dieser* τ *Werthe von* r *gehören* δ *verschiedene und* δ *andere Werthe von* z. *Oder mit andern Worten: die Gleichung* (1.) *hat für jeden der* τ *verschiedenen Werthe, die* r *haben kann,* δ, *und für jedes* r, δ *andere Wurzeln.*

II. *Unter den* τ *verschiedenen Werthen, welche* r *in* (1.) *haben kann, ist immer und für jedes* δ *auch der Werth* $r = 1$, *und er ge-*

hört ***immer*** *zu* $z=1$. *Ist* δ *gerade, so gehört* $r=1$ *zugleich zu* $z=p-1$, *und ist* δ ***ungerade***, *so gehört zu* $z=p-1$ *der Rest* $r=p-1$ *oder* $r=-1$.

III. *Für* $\delta=p-1$, *also* $\tau=1$, *kann* r ***nur*** $=1$ *sein, und in diesem Fall drückt die Gleichung* (1.) *den Fermatschen Lehrsatz* (§. 40.) *aus. Es ist also von diesem Satze der gegenwärtige auf gewisse Weise eine* ***Erweiterung***.

IV. *Für* $\delta=\frac{1}{2}(p-1)$, *also* $\tau=2$, *hat* r ***nur*** *die beiden Werthe* 1 *und* $p-1$ *oder* $=+1$ *und* -1, *und die zu* $r=+1$ *gehörigen* z *sind die* ***Quadratreste***, *die zu* $r=-1$ *gehörigen* z *die* ***Nichtquadratreste*** *zu* p.

V. *Ferner ist*

$$6.\quad (p-z)^\delta = \mathfrak{G}p+r,\quad \textit{wenn } \delta \textit{ gerade und}$$

$$7.\quad (p-z)^\delta = \mathfrak{G}p-r,\quad \textit{wenn } \delta \textit{ ungerade ist.}$$

Das heifst, wenn δ ***gerade*** *ist geben* z *und* $p-z$ ***gleiche*** *Reste, und wenn* δ ***ungerade*** *ist, sind die Reste, welche* z *und* $p-z$ *geben,* ***zusammen*** $=p$.

VI. *Von den* δ *verschiedenen Werthen von* z, *welche in* (1.) *einen und denselben Rest* r *geben, lassen in* (2.) *je* $\varkappa$ ***verschiedene*** *Reste* ϱ, *und je* λ *der Reste* ϱ *sind für ein und dasselbe* r *einander gleich.*

Beispiele. Die weiter unten angehängte, mit I. bezeichnete Tafel, welche die sämmtlichen Reste der 1, 2, 3, 4, ... 60 ($=p-1$)ten Potenzen von den Zahlen 1, 2, 3, 4, ... $=60$ zu der Stammzahl $p=61$ enthält, liefert Beispiele zu dem gegenwärtigen und zugleich zu den folgenden Lehrsätzen. Wie solche Tafel mit verhältnifsmäfsig geringer Mühe zu berechnen sei, wird sich weiter unten zeigen.

Zu I. $\delta=4$ geht in $p-1=60$ auf und giebt $\tau=15$ (3.). Die Tafel zeigt, dafs für den Exponenten $\delta=4$, r die $\tau=15$ verschiedenen Werthe 1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57 und 58 hat und dafs jeder dieser Werthe von r, $\delta=4$ mal vorkommt.

$\delta=10$ geht in $p-1=60$ auf und giebt $\tau=6$ (3.), und für den Exponenten $\delta=10$ hat nach der Tafel r die $\tau=6$ verschiedenen Werthe 1, 13, 14, 47, 48 und 60; jeder dieser Werthe von r kommt $\delta=10$ mal vor.

Zu II. Für *jedes* δ gehört zu $z=1$ der Rest $r=1$. Für alle *geraden* δ gehört zu $z=p-1=60$ der Rest $r=1$ und für alle *ungeraden* δ der Rest $r=p-1=60$ oder $r=-1$.

Zu III. Für $\delta = p - 1 = 60$ sind *alle* r gleich 1; dem Fermatschen Lehrsatze gemäfs.

Zu IV. Für $\delta = 30 = \frac{1}{2}(p-1)$ hat r, wie die Tafel zeigt, nur die beiden Werthe 1 und $p - 1 = 60$. Die zu $r = +1$ gehörigen 30 Werthe

8. 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58 und 60

von z sind die Werthe von r für $\delta = 2$ in der zweiten horizontalen Reihe, also die *Quadratreste* zu p. Die zu $r = p - 1 = 60$ für $\delta = 30$ gehörigen z sind die *übrigen* 30 Zahlen, welche diejenigen (8.) von den Zahlen 1, 2, 3, 4, ... 60 noch übrig lassen, also die *Nichtquadratreste* zu p.

Zu V. Für das *gerade* $\delta = 14$ z. B. giebt nach der Tafel $z = 19$ den Rest $r = 16$ und $p - z = 61 - 19 = 42$ giebt *ebenfalls* den Rest $r = 16$. Für das gerade $\delta = 52$ giebt $z = 26$ den Rest $r = 57$ und $p - z = 61 - 26 = 35$ giebt *ebenfalls* den Rest $r = 57$.

Für das *ungerade* $\delta = 21$ giebt $z = 12$ den Rest $r = 34$ und $p - z = 61 - 12 = 49$ giebt den Rest $r = 27 = p - 34$. Für das ungerade $\delta = 9$ giebt $z = 16$ den Rest $r = 58$ und $p - z = 61 - 16 = 45$ giebt den Rest $r = 3 = p - 58$.

Zu VI. Für $\delta = 20$, also $\tau = 3$ (3.), hat der Rest r die $\tau = 3$ Werthe 1, 13 und 47, und z. B. den Rest $r = 13$ geben die $\delta = 20$ Werthe

9. 4, 10, 12, 14, 17, 19, 25, 26, 29, 30, 31, 32, 35, 36, 42, 44, 47, 49, 51 und 57 von z.

Setzt man nun $\lambda = 4$, so ist $x = 5$ (4.), und sucht man die Reste zur $\lambda = 4$ten Potenz der Werthe (9.) von z auf, so ergiebt sich, dafs

10.
- die $\lambda = 44$ Werthe 4, 17, 4 und 57 von z den Rest $\rho = 12$,
- - $\lambda = 4$ - - 10, 12, 49 und 51 von z - - $\rho = 57$,
- - $\lambda = 4$ - - 14, 29, 32 und 47 von z - - $\rho = 47$,
- - $\lambda = 4$ - - 19, 26, 35 und 42 von z - - $\rho = 25$,
- und die $\lambda = 4$ - - 25, 30, 31 und 36 von z - - $\rho = 42$

lassen, also je $\lambda = 4$ der $\delta = 20$ Werthe (9.) von z, die in (1.) zu *einem und demselben* Rest $r (= 13)$ gehören, in (2.) $x = 5$ verschiedene Reste $\rho = 12, 57, 47, 25$ und 42; gemäfs (VI.).

Beweis A. Nimmt man von (1.) die τte Potenz, so ergiebt sich

11. $z^{\delta\tau} = (\mathfrak{G}p + r)^\tau = \mathfrak{G}p + r^\tau$ (§. 12. 20.),

und da $\vartheta_r = p-1$ (2.), z^{p-1} aber nach (§. 40.) $= \mathfrak{G}p+1$ ist, $\mathfrak{G}p+1 = \mathfrak{G}p+r^\tau$ oder

$$12. \quad r^\tau = \mathfrak{G}p+1.$$

B. Nun ist aber auch eben so wohl, dem Fermatschen Satze zufolge,

$$13. \quad r^{p-1} = \mathfrak{G}p+1;$$

denn r ist jedenfalls eine der Zahlen (5.), welche z sein kann.

Aus (12. und 13.) folgt

$$14. \quad r^\tau - 1 = \mathfrak{G}p \quad \text{und} \quad r^{p-1} - 1 = \mathfrak{G}p.$$

Da nun τ in $p-1$ *aufgeht*, so geht auch $r^\tau - 1$, wenn man damit $r^{p-1}-1$ dividirt, darin auf und es ist

$$15. \quad r^{p-1}-1 = (r^\tau-1)(r^{(\vartheta-1)\tau}+r^{(\vartheta-2)\tau}+r^{(\vartheta-3)\tau}\ldots\ldots+1) = \mathfrak{G}p.$$

C. In $r^{p-1}-1 = \mathfrak{G}p$ hat, dem Fermatschen Satze zufolge, r *nothwendig alle* die $p-1$ verschiedenen Werthe $1, 2, 3, 4, \ldots\ldots p-1$: also mufs für *alle* diese Werthe von r auch nothwendig das *Product* rechterhand in (15.) mit p aufgehen.

D. Es kann aber der Factor $r^\tau-1$ in (15.) für *nicht mehr* als τ verschiedene Werthe von r, und der Factor $r^{(\vartheta-1)\tau}+r^{(\vartheta-2)\tau}+r^{(\vartheta-3)\tau}\ldots\ldots+1$ für *nicht mehr* als $(\vartheta-1)\tau$ verschiedene Werthe von r mit p aufgehen. Denn die Gleichungen

$$16. \quad r^\tau - 1 = \mathfrak{G}p \quad \text{und}$$

$$17. \quad r^{(\vartheta-1)\tau}+r^{(\vartheta-2)\tau}+r^{(\vartheta-3)\tau}\ldots\ldots+1 = \mathfrak{G}p$$

können dem Lehrsatze (§. 44.) zufolge, erstere *nicht mehr* als τ, letztere *nicht mehr* als $(\vartheta-1)\tau$ verschiedene Wurzeln haben.

Daraus, und dafs nach (*C.*) die beiden Gleichungen (16. und 17.) *zusammen* nothwendig $p-1$ verschiedene Wurzeln haben *müssen*, folgt, dafs die Gleichung (16.) nothwendig *gerade* τ verschiedene Wurzeln haben *mufs*, und die Gleichung (17.) die übrigen $(\vartheta-1)\tau$ Wurzeln. Denn hätte (16.) *weniger* als τ Wurzeln, so müfste (17.) eben so viele Wurzeln *mehr* als $(\vartheta-1)\tau$ haben, indem $\tau+(\vartheta-1)\tau = \vartheta\tau = p-1$ ist; was nach (§. 44.) nicht möglich ist. So kann also (16.) *nicht weniger* als τ Wurzeln haben, und nach (§. 44.) auch *nicht mehr:* also mufs die Zahl der Wurzeln von (16.) nothwendig *gleich* τ sein. Auch können (16. und 17.) nicht etwa Wurzeln *gemeinschaftlich* haben. Denn hätte z. B. (16.) σ Wurzeln mit (17.) gemeinschaftlich, so könnten in (16. und 17.) überhaupt nur $p-1-\sigma$ *verschiedene* Wurzeln vorkommen, da (16. und 17.) *zusammen* nur $\tau+(\vartheta-1)\tau = p-1$ Wurzeln haben können: gleichwohl müssen in (16. und 17.) zusam-

men *alle* die verschiedenen $p-1$ Werthe $1, 2, 3, 4, \dots p-1$ von r vorkommen, weil dies in (13.) der Fall ist.

Es hat also nothwendig in (12.), und folglich in (11.), woraus (12.) folgt, und mithin auch in (1.), woraus (11.) folgt, der Rest r, τ und *nur* τ verschiedene Werthe > 0 und $< p$. Dieses ist was zunächst der Lehrsatz in (I.) behauptet.

E. Es folgt ferner aus

$$18. \quad z^{p-1} = \mathfrak{G}p + 1 \ (\text{§. } 40.) \text{ und}$$

$$19. \quad r^{\tau} = \mathfrak{G}p + 1 \ (12.),$$

wenn man (19.) von (18.) abzieht,

$$20. \quad z^{p-1} - r^{\tau} = \mathfrak{G}p.$$

Aber τ geht in $p-1$ auf, denn es ist $p-1 = \delta\tau$ (3.). Daher geht auch $z^{p-1} - r^{\tau}$ mit $z^{\delta} - r$ *auf* und man erhält, wenn man dividirt, statt (20.):

$$21. \quad z^{\delta\tau} - r^{\tau} = (z^{\delta} - r)(z^{\delta(\tau-1)} + z^{\delta(\tau-2)} r + z^{\delta(\tau-3)} r^2 \dots + z^{2\delta} r^{\tau-2} + z^{\delta} r^{\tau-2} + r^{\tau-1}) = \mathfrak{G}p;$$

nemlich, in (21.) die Factoren wiederum multiplicirt, giebt

$$22. \quad \begin{aligned} & z^{\delta\tau} + z^{\delta(\tau-1)} r + z^{\delta(\tau-2)} r^2 \dots + z^{3\delta} r^{\tau-3} + z^{2\delta} r^{\tau-2} + z^{\delta} r^{\tau-1} \\ & - z^{\delta(\tau-1)} r - z^{\delta(\tau-2)} r^2 \dots\dots \quad \dots\dots - z^{2\delta} r^{\tau-2} - z^{\delta} r^{\tau-1} - r^{\tau} \\ & = z^{\delta\tau} - r^{\tau}. \end{aligned}$$

F. Da nun die Gleichung (18.) für alle die $p-1$ verschiedenen Werthe $1, 2, 3, 4, \dots p-1$ von z gilt, so mufs auch (21.) *alle* diese Werthe von z zulassen, und folglich müssen die beiden Factoren rechterhand in (21.) für *alle* diese verschiedenen Werthe von z mit p aufgehen.

G. Ganz so wie in (*D.*) folgte, dafs die beiden Factoren rechterhand in (15.) nothwendig, der eine τ, der andere $(\delta-1)\tau$ verschiedene Werthe von r zulassen müssen, folgt auch hier, dafs die beiden Factoren rechterhand in (21.), der eine nothwendig für δ, der andere für $\delta(\tau-1)$ verschiedene Werthe von z gelten müssen, denn die Gleichungen

$$23. \quad z^{\delta} - r = \mathfrak{G}p \text{ und}$$

$$24. \quad z^{\delta(\tau-1)} + z^{\delta(\tau-2)} r + z^{\delta(\tau-3)} r^2 \dots + z^{2\delta} r^{\tau-3} + z^{\delta} r^{\tau-2} + r^{\tau-1} = \mathfrak{G}p$$

können nach (§. 44.), die erste *nicht mehr* als δ, die zweite *nicht mehr* als $\delta(\tau-1)$ verschiedene Wurzeln haben.

Also folgt aus der Gleichung (23.), welche diejenige (1.) selbst ist, dafs zu jedem Werth, welchen r haben kann, und deren es nach (*D.*) τ giebt,

z nothwendig δ verschiedene Werthe hat. Und zwar müssen jedem ***andern r***, ***δ andere z*** entsprechen: denn gehörten zu ***verschiedenen r gleiche z***, so würden, indem nur τ verschiedene r vorhanden sind, ***nicht alle*** $p-1=\delta\tau$ verschiedene Werthe von z vorkommen; was gleichwohl in (21.) oder (18.) der Fall sein mufs.

Dieses ist was der Lehrsatz weiter in (I.) behauptet.

H. Für *jedes* δ giebt in (1.) $z=1$, $r=1$. Für jedes *gerade* δ giebt (1.) $(p-1)^\delta=\mathfrak{S}p+1$, also $r=1$; für jedes *ungerade* δ giebt (1.) $(p-1)^\delta=\mathfrak{S}p-1$, also $r=p-1$ oder $r=-1$. Dieses ist was (II.) behauptet.

I. Für $\delta=p-1$ giebt (1.), dem Fermatschen Lehrsatze (§. 40.) gemäfs, für *jedes z*, $z^{p-1}=\mathfrak{S}p+1$; gemäfs (III.).

K. Für $\delta=\frac{1}{2}(p-1)$ giebt (1.), wenn man für z die *Quadratreste* zu p setzt, zufolge (§. 49.), $z^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$, und wenn man für z die *Nichtquadratreste* zu p setzt, zufolge (§. 49. 2.), $z^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$; gemäfs (IV.).

L. Setzt man in (1.) $p-z$ statt z, so ergiebt sich

25. $$(p-z)^\delta = \mathfrak{S}p+(-z)^\delta = \mathfrak{S}p\pm(\mathfrak{S}p+r)\,(1.) = \mathfrak{S}p\pm r,$$

je nachdem δ *gerade* oder *ungerade* ist; gemäfs (6. und 7. V.).

M. Aus (2.) folgt, wenn man die $x$ten Potenzen davon nimmt,

26. $$z^{x\lambda} = \mathfrak{S}p+\varrho^x = z^\delta\ (4.),$$

also ist, gemäfs (1.),

$$\mathfrak{S}p+r = \mathfrak{S}p+\varrho^x \text{ oder}$$

27. $$\varrho^x = \mathfrak{S}p+r,$$

mithin hat ϱ, zufolge (I.), für ***ein*** und ***dasselbe r***, ***x verschiedene*** Werthe aus denen von z, welche in (1.) das bestimmte r geben. Andrerseits gehören in (2.), ebenfalls gemäfs (I.), λ verschiedene Werthe von z zu einem und demselben ϱ; und da nun alle die Werthe von ϱ aus denjenigen Werthen von z sind, die in (1.) ein und dasselbe r geben, so gehören λ ***dieser*** Werthe von z zu einem und demselben r. Dieses zusammen behauptet (VI.).

Anm. *N.* Der Beweis beruht auf einer Verbindung der Sätze (§. 40. 43. und 44.). Wie in (§. 51.) sind hier die Schlüsse in (*D.* und *G.*) eigenthümlich.

§. 55.

Lehrsatz.

Es sei in den Zahlengleichungen

$$1. \quad z^{\varepsilon} = \mathfrak{G}p + r \quad \textit{und}$$

$$2. \quad z^{\sigma} = \mathfrak{G}p + \varrho$$

p *eine Stammzahl,* $r > 0$ *und* $< p$ *und der Reihe nach*

$$3. \quad z = 1, 2, 3, 4, \ldots\ldots p-1.$$

I. *Sind in* (1.) *und* (2.) ε *und* σ *zu einander theilerfremd, gleichviel ob auch zu* $p-1$, *oder nicht, so geben diejenigen Werthe von* z *aus denen* (3.), *zu welchen in* (1.) *gleiche* r *gehören, in* (2.) *nicht zugleich gleiche* ϱ; *und umgekehrt.*

II. *Ist in* (1.) ε *zu* $p-1$ *theilerfremd, so bekommt* r *zu jedem andern Werth von* z *einen andern Werth, und die Werthe von* r *durchlaufen, eben wie* z *selbst, alle die Zahlen* 1, 2, 3, 4, ... $p-1$, *obwohl in verschiedener Ordnung.*

III. *Ferner ist in* (1.)

$$4. \quad (p-z)^{\varepsilon} = \mathfrak{G}p + r \quad \textit{für gerade } \varepsilon \textit{ und}$$

$$5. \quad (p-z) = \mathfrak{G}p - r \quad \textit{für ungerade } \varepsilon;$$

das heifst, wenn z *zu* p *den Rest* r *läfst, so gehört für ein gerades* ε *zu* $p-z$ *derselbe Rest* r *und für ein ungerades* ε *der Rest* $-r$ *oder* $p-r$.

IV. *Ist* δ *der gröfste Gemeintheiler von* ε *und* $p-1$ *und*

$$6. \quad \varepsilon = \eta\delta, \quad p-1 = \tau\delta,$$

so bekommt r *in* (1.) *je für* δ *und für nicht mehrere verschiedene Werthe von* z *aus denen* (3.) *denselben Werth, und für die sämmtlichen* z (3.) τ *verschiedene Werthe.*

V. *Ist* λ *irgend ein Gemeintheiler von* ε *und* σ *und zugleich ein Theiler von* $p-1$, *z. B.*

$$7. \quad \varepsilon = x\lambda, \quad \sigma = \omega\lambda \quad \textit{und} \quad p-1 = \zeta\lambda,$$

so gehören zu den nemlichen je λ *Werthen von* z *aus denen* (3.), *welche in* (1.) *gleiche* r *geben, auch in* (2.) *gleiche* ϱ, *und in dem Fall, wenn* x *und* ω *zu einander theilerfremd sind, nicht mehrere.*

Beispiele (aus Taf. I.). Zu I. $\sigma = 21$ und $\varepsilon = 50$ sind zu einander *theilerfremd*, aber beide *nicht* zu $p-1 = 60$. Die 3 Werthe 7, 24 und 30 von z, welche für $\sigma = 21$ den Rest $\varrho = 24$ lassen, geben für $\varepsilon = 50$ die Reste $r = 14$, 60 und 48, also *andere* Reste; gemäfs (I.).



$\sigma = 18$ und $\varepsilon = 49$ sind zu einander *theilerfremd*, aber nur ε ist es zugleich zu $p-1=60$. Die 6 Werthe 4, 5, 9, 52, 56 und 57 von z, welche für $\sigma = 18$ den Rest $\varrho = 58$ lassen, geben für $\varepsilon = 49$ die Reste 49, 46, 34, 27, 15 und 12, also *andere* Reste; gemäfs (I.).

$\sigma = 13$ und $\varepsilon = 49$ sind zu einander und zugleich *beide* zu $p-1=60$ *theilerfremd*. Der Werth 3 von z, welcher für $\sigma = 13$ den Rest $\varrho = 27$ läfst, giebt für $\varepsilon = 49$ den Rest $r = 41$, also einen *andern* Rest; gemäfs (I.).

Zu II. Die Zahlen

8. $\varepsilon = 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53$ und $59 > 1$

sind zu $p-1=60$ *theilerfremd;* und für *alle* diese Werthe ε des Exponenten der z in (1.) hat r, wie es die Tafel zeigt, für jeden andern Werth von z einen *andern* Werth. Die Werthe von r durchlaufen, eben wie die z selbst, alle die Zahlen 1, 2, 3, 4, ... $p-1$, obwohl in verschiedener Ordnung; gemäfs (II.).

Zu III. Für das *gerade* $\varepsilon = 38$ ist z. B. für $z = 13$, $r = 47$, und für $z = 48 = p-13$ ist r ebenfalls $= 47$; gemäfs (4.).

Für das *ungerade* $\varepsilon = 53$ ist z. B. für $z = 16$, $r = 57$ und für $z = 45 = p - 16$ ist $r = 4 = p - 57$; gemäfs (5.).

Zu IV. Es sei $\varepsilon = 42$, so ist der gröfste Gemeintheiler von ε in $p-1=60$, $\delta = 6$ und in (6.) $\eta = 7$, $\tau = 10$. In der Tafel findet sich, dafs für die εte $= 42$te Potenz der z, z. B. die $\delta = 6$ Werthe 3, 19, 22, 38, 42 und 51 von z einen und denselben Rest $r = 9$ geben: und für die sämmtlichen z (3.) hat r die $\tau = 10$ verschiedenen Werthe 1, 3, 9, 20, 27, 34. 41, 52, 58 und 60; gemäfs (IV.).

Zu V. Der Gemeintheiler $\lambda = 6$ zu $\varepsilon = 24$ und $\sigma = 48$ ist zugleich ein Theiler von $p-1=60$. Die $\lambda = 6$ Werthe 4, 5, 6, 9, 17, 23 von z geben für $\varepsilon = 24$ den Rest $r = 34$. *Dieselben* Werthe von z geben zu $z^\varepsilon = z^\sigma$ alle den Rest $\varrho = 58$; gemäfs (V.).

Ein Gemeintheiler zu $\varepsilon = 24$ und $\sigma = 45$ ist $\lambda = 3$, was zugleich in $p-1=60$ aufgeht. Dabei ist $x = 8$ und $\omega = 15$, und diese Werthe von x und ω sind zu einander *theilerfremd*. Die 12 Werthe 2, 3. 19, 22, 26, 28. 33, 35, 39, 42, 58 und 59 von z geben für $\varepsilon = 24$ den Rest $\varrho = 20$ und für $\sigma = 45$ die Reste 50, 60, 60, 1. 50, 11, 50. 11, 60, 1, 1 und 11, und nur je $\lambda = 3$ von den letztern sind wieder gleich: gemäfs (V.).

Beweis A. Von den beiden Exponenten ε und σ in (1. und 2.) bezeichne ε den *grössern*. Man setze

$$9.\quad \begin{cases} \varepsilon = m\sigma + \sigma_1, \\ \sigma = m_1\sigma_1 + \sigma_2, \\ \sigma_1 = m_2\sigma_2 + \sigma_3, \\ \sigma_2 = m_3\sigma_3 + \sigma_4, \\ \dots\dots\dots\dots \\ \sigma_{n-2} = m_{n-1}\sigma_{n-1} + \sigma_n, \end{cases}$$

wo $\sigma_1 < \sigma$, $\sigma_2 < \sigma_1$, $\sigma_3 < \sigma_2$, ... sein sollen.

a. Da ε und σ zu einander *theilerfremd* sein sollen, so führt (9.) nach (§. 19. IV.) *nothwendig* zuletzt auf den Rest $\sigma_n = 1$.

b. Es seien a und b zwei von den Werthen von z, welche nach der Voraussetzung in (1.) *gleiche Reste* r lassen, so dafs also

$$10.\quad a^\varepsilon = \mathfrak{S}p + r \quad \text{und} \quad b^\varepsilon = \mathfrak{S}p + r$$

ist. Könnten nun diese *nemlichen* Werthe a und b von z auch in (2.) *gleiche* Reste ϱ lassen, so müfste auch

$$11.\quad a^\sigma = \mathfrak{S}p + \varrho \quad \text{und} \quad b^\sigma = \mathfrak{S}p + \varrho$$

sein.

c. Drückt man in (10.) ε nach der ersten der Gleichungen (9.) aus, so ergiebt sich

$$a^{m\sigma+\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad b^{m\sigma+\sigma_1} = \mathfrak{S}p + r \quad \text{oder}$$

$$12.\quad a^{m\sigma}a^{\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad b^{m\sigma}b^{\sigma_1} = \mathfrak{S}p + r,$$

und da nach (11.)

$$13.\quad a^{m\sigma} = \mathfrak{S}p + \varrho^m \quad \text{und} \quad b^{m\sigma} = \mathfrak{S}p + \varrho^m$$

ist (§. 12. 20.),

$$(\mathfrak{S}p + \varrho^m)a^{\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad (\mathfrak{S}p + \varrho^m)b^{\sigma_1} = \mathfrak{S}p + r \quad \text{oder}$$

$$14.\quad \varrho^m a^{\sigma_1} = \mathfrak{S}p + r \quad \text{und} \quad \varrho^m b^{\sigma_1} = \mathfrak{S}p + r.$$

d. Die Gleichungen (14.) von einander abgezogen, geben

$$15.\quad \varrho^m(a^{\sigma_1} - b^{\sigma_1}) = \mathfrak{S}p,$$

oder, wenn man

$$16.\quad a^{\sigma_1} = \mathfrak{S}p + a_1 \quad \text{und} \quad b^{\sigma_1} = \mathfrak{S}p + b_1$$

setzt, wo $a_1 < p$ und $b_1 < p$ angenommen wird,

$$\varrho^m(\mathfrak{S}p + a_1 - \mathfrak{S}p - b_1) = \mathfrak{S}p \quad \text{oder}$$

$$17.\quad \varrho^m(a_1 - b_1) = \mathfrak{S}p:$$

also müfste entweder ϱ oder $a_1 - b_1$ mit p *aufgehen*. Da beides nicht der Fall ist, indem ϱ, a, und b_1 alle drei $< p$ sind, so kann die Gleichung (17.)

nur erfüllt werden, wenn $a_1 - b_1 = 0$ oder

$$18.\quad a_1 = b_1$$

ist. Folglich können die beiden Werthe a und b von z, die nach der Voraussetzung in (1.) *gleiche* Reste r lassen, nur dann auch in (2.) *gleiche* Reste ϱ geben, wenn in (16.) $a_1 = b_1$ ist.

e. Die Gleichungen (11.), nach der zweiten Gleichung in (9.) ausgedrückt, geben

$$a^{m_1\sigma_1+\sigma_2} = \mathfrak{S}p + \varrho \quad \text{und} \quad b^{m_1\sigma_1+\sigma_2} = \mathfrak{S}p + \varrho \quad \text{oder}$$

$$19.\quad a^{m_1\sigma_1}a^{\sigma_2} = \mathfrak{S}p + \varrho \quad \text{und} \quad b^{m_1\sigma_1}b^{\sigma_2} = \mathfrak{S}p + \varrho,$$

oder, da vermöge (16.)

$$20.\quad a^{m_1\sigma_1} = \mathfrak{S}p + a_1^{m_1} \quad \text{und} \quad b^{m_1\sigma_1} = \mathfrak{S}p + b_1^{m_1}$$

ist (§. 12. 20.),

$$(\mathfrak{S}p + a_1^{m_1})a^{\sigma_2} = \mathfrak{S}p + \varrho \quad \text{und} \quad (\mathfrak{S}p + b_1^{m_1})b^{\sigma_2} = \mathfrak{S}p + \varrho \quad \text{oder}$$

$$21.\quad a_1^{m_1}a^{\sigma_2} = \mathfrak{S}p + \varrho \quad \text{und} \quad b_1^{m_1}b^{\sigma_2} = \mathfrak{S}p + \varrho,$$

oder auch, da nach (18.) $a_1 = b_1$ sein mufs,

$$22.\quad a_1^{m_1}a^{\sigma_2} = \mathfrak{S}p + \varrho \quad \text{und} \quad a_1^{m_1}b^{\sigma_2} = \mathfrak{S}p + \varrho.$$

f. Die Gleichungen (22.) von einander abgezogen, geben

$$23.\quad a_1^{m_1}(a^{\sigma_2} - b^{\sigma_2}) = \mathfrak{S}p,$$

oder, wenn man

$$24.\quad a^{\sigma_2} = \mathfrak{S}p + a_2 \quad \text{und} \quad b^{\sigma_2} = \mathfrak{S}p + b_2$$

setzt, wo $a_2 < p$ und $b_2 < p$ angenommen wird,

$$a_1^{m_1}(\mathfrak{S}p + a_2 - \mathfrak{S}p - b_2) = \mathfrak{S}p \quad \text{oder}$$

$$25.\quad a_1^{m_1}(a_2 - b_2) = \mathfrak{S}p:$$

also müfste entweder a_1 oder $a_2 - b_2$ mit p *aufgehen*. Da beides nicht der Fall ist, indem a_1, a_2 und b_2 alle drei $< p$ sind, so kann die Gleichung (25.) nur erfüllt werden, wenn $a_2 - b_2 = 0$ oder

$$26.\quad a_2 = b_2$$

ist. Folglich können die beiden Werthe a und b von z, die nach der Voraussetzung (in 1.) *gleiche* Reste r lassen, nur dann auch in (2.) *gleiche* Reste ϱ geben, wenn, nächst $a_1 = b_1$ in (16.), auch in (24.) $a_2 = b_2$ ist.

g. Die Gleichungen (16.) sind, da $a_1 = b_1$ sein mufs (18.),

$$27.\quad a^{\sigma_1} = \mathfrak{S}p + a_1 \quad \text{und} \quad b^{\sigma_1} = \mathfrak{S}p + a_1.$$

Verfährt man mit diesen Gleichungen von neuem ganz so wie in (*c.* und *d.*) mit den Gleichungen (11.), und zwar indem man den Exponenten σ_1 in (27.) nach der *dritten* Gleichung (9.) ausdrückt, so ergiebt sich, wie leicht zu sehen, indem nur alle *Zeiger* um 1 erhöht werden dürfen, dafs, wenn man,

ähnlich wie in (24.),

$$28.\quad a^{\sigma_3} = \mathfrak{G}p + a_3 \quad \text{und} \quad b^{\sigma_3} = \mathfrak{G}p + b_3$$

setzt, auch wieder, ähnlich wie in (26.),

$$29.\quad a_3 = b_3$$

sein mufs, wenn die Gleichungen (27.) und folglich die Gleichungen (11.) Statt finden sollen.

h. Auf dieselbe Weise folgt weiter, dafs

$$30.\quad \begin{cases} \text{Für } a^{\sigma_4} = \mathfrak{G}p + a_4 \text{ und } b^{\sigma_4} = \mathfrak{G}p + b_4,\ a_4 = b_4; \\ \text{Für } a^{\sigma_5} = \mathfrak{G}p + a_5 \text{ und } b^{\sigma_5} = \mathfrak{G}p + b_5,\ a_5 = b_5; \\ \quad \text{und so weiter; zuletzt also dafs} \\ \text{Für } a^{\sigma_n} = \mathfrak{G}p + a_n \text{ und } b^{\sigma_n} = \mathfrak{G}p + b_n,\ a_n = b_n \end{cases}$$

sein mufs, wenn die Gleichungen (11.) Statt finden sollen, das heifst, wenn zwei Werthe a und b von z, die in $z^\varepsilon = \mathfrak{G}p + r$ (1.) *gleiche* Reste r zu p lassen, auch in $z^\sigma = \mathfrak{G}p + \varrho$ (2.) zu p *gleiche* Reste ϱ geben sollen.

i. Nun ist aber $\sigma_n = 1$ (*a.*), also geben die letzten der Gleichungen (30.)

$$a^1 = \mathfrak{G}p + a_n \quad \text{und} \quad b^1 = \mathfrak{G}p + b_n \quad \text{oder}$$

$$31.\quad a_n = a \quad \text{und} \quad b_n = b.$$

Die letzte Bedingung $a_n = b_n$ in (30.) für das Stattfinden der Gleichungen (11.) wäre also

$$32.\quad a = b.$$

Diese Bedingung wird *nicht* erfüllt, indem a und b nicht *gleiche* sondern *ungleiche* Werthe von z ausdrücken. Also können die Gleichungen (11.) *nicht* Statt finden: das heifst, keine zwei Werthe a und b von z, und folglich auch überhaupt nicht diejenigen Werthe von z, welche in $z^\varepsilon = \mathfrak{G}p + r$ (1.) zu p *gleiche* Reste r lassen, können zugleich in $z^\sigma = \mathfrak{G}p + \varrho$ (2.) zu p *gleiche* Reste ϱ geben, sobald ε und σ zu einander *theilerfremd* sind. Ob ε und σ zu $p-1$ theilerfremd sind, oder nicht, kommt bei dem Beweise nicht in Betracht.

Dieses ist es, was der Lehrsatz in (I.) behauptet.

B. Wenn in (2.) $\sigma = p - 1$ ist, so geben *alle* die Werthe (3.) von z nach dem Fermatschen Lehrsatze (§. 40.) *gleiche* Reste ϱ, nemlich *alle* den Rest $\varrho = 1$. Nun geben nach (I.) alle die Werthe von z, die in (2.) *gleiche* Reste ϱ lassen, in (1.) *nicht* gleiche Reste r. Also geben in dem gegenwärtigen Fall *alle* die Werthe (3.) von z in (1.) sämmtlich *verschiedene* Werthe von r. Und folglich mufs, da $p-1$ Werthe von z und folglich von r vorhanden und alle >0 und $<p$ sind, r, eben wie z, alle die Zahlen (3.) durchlaufen. Dies behauptet (II.).

C. Es ist

$$33. \quad (p-z)^\varepsilon = \mathfrak{G}p + (-z)^\varepsilon = \mathfrak{G}p + z^\varepsilon(-1)^\varepsilon$$

und, da $z^\varepsilon = \mathfrak{G}p + r$ ist (1.),

$$34. \quad (p-z)^\varepsilon = \mathfrak{G}p + (\mathfrak{G}p + r)(-1)^\varepsilon = \mathfrak{G}p + r(-1)^\varepsilon.$$

Dieses giebt

$$35. \quad (p-z)^\varepsilon = \mathfrak{G}p + r, \text{ wenn } \varepsilon \textit{ gerade} \text{ und}$$

$$36. \quad (p-z)^\varepsilon = \mathfrak{G}p - r, \text{ wenn } \varepsilon \textit{ ungerade} \text{ ist;}$$

gemäfs (III.).

D. a. Setzt man für (IV.), wo δ einer der Theiler von $p-1$ sein soll,

$$37. \quad z^\delta = \mathfrak{G}p + r_1,$$

so geben nach (§. 54. I.) δ verschiedene Werthe von z, und nicht mehrere, *denselben* Rest r_1.

Da nun $\eta\delta = \varepsilon$ sein soll (6.), so giebt (37.)

$$38. \quad z^{\eta\delta} \text{ oder } z^\varepsilon = \mathfrak{G}p + r_1^\eta \text{ (§. 12. 20.)}$$

und, da $z^\varepsilon = \mathfrak{G}p + r$ sein soll (1.),

$$\mathfrak{G}p + r = \mathfrak{G}p + r_1^\eta \text{ oder}$$

$$39. \quad r_1^\eta = \mathfrak{G}p + r.$$

Nun geben δ verschiedene und nicht mehrere Werthe von z in (37.) *denselben* Rest r_1, also geben sie auch vermöge (39.) denselben Werth r für (2.).

b. Aber obgleich nicht mehre als δ Werthe von z in (37.) denselben Rest r_1 lassen, fragt es sich doch, ob nicht dennoch etwa andere Werthe von z nach (39.) für (1.) gleiche Reste r geben.

Andere als diejenigen δ Werthe von z, welche in (37.) dasselbe r_1 geben, lassen nothwendig in (37.) einen *andern* Rest r_2, so dafs für sie

$$40. \quad z^\delta = \mathfrak{G}p + r_2$$

ist. Sollte nun dieser Werth von z dennoch in (2.) denselben Rest r lassen, so müfste gemäfs (39.)

$$41. \quad r_2^\eta = \mathfrak{G}p + r$$

sein; also müfste die ηte Potenz zweier *verschiedenen* Zahlen r_1 und r_2, beide >0 und $<p$, zu p den *gleichen* Rest r lassen. Dieses aber ist nach (II.) nicht möglich, indem δ der *gröfste* Gemeintheiler von ε und $p-1$ sein soll, also η zu $p-1$ *theilerfremd* ist. Also lassen *nicht mehr* als δ verschiedene Werthe von z in (1.) *denselben* Rest r, sobald δ der *gröfste* Gemeintheiler von ε und $p-1$ ist. Mithin giebt es dann auch in (1.) in diesem

Falle nur $\frac{p-1}{\delta} = \tau$ (6.) *verschiedene* Werthe von r. Dieses zusammen behauptet (IV.).

E. *a.* In (V.) soll λ ein Theiler von $p-1$ sein. Dieserhalb geben zufolge (§. 54. I.), wenn man

$$42. \quad z^{\lambda} = \mathfrak{G}p + r_1$$

setzt, λ verschiedene Werthe von z das *gleiche* r_1.

Da nun $\varepsilon = x\lambda$ und $\sigma = \omega\lambda$ sein soll (7.), so giebt (42.)

$$43. \quad z^{x\lambda} \text{ oder } z^{\varepsilon} = \mathfrak{G}p + r_1^{x} = \mathfrak{G}p + r \text{ (1.) und}$$

$$44. \quad z^{\omega\lambda} \text{ oder } z^{\sigma} = \mathfrak{G}p + r_1^{\omega} = \mathfrak{G}p + \varrho \text{ (2.);}$$

und folglich sind für je λ verschiedene Werthe von z die Werthe von r_1^{x} und r_1^{ω} und folglich von r in (1.) und ϱ in (2.) einander gleich.

b. Sind x und ω zu einander *theilerfremd*, so folgt, eben wie in (*D.* *b.*), dafs nicht auch noch andere als die λ Werthe von z in (1. und 2.) ebenfalls gleiche r und *zugleich* gleiche ϱ geben können.

F. Anm. Ein Hauptmoment des Beweises ist (*A.*), nemlich, dafs man, wenn ε und σ zu einander *theilerfremd* sind, nach (§. 19. IV.) nothwendig auf den Rest $\sigma_n = 1$ kommt. Sonst beruht der Beweis auf (§. 40. und 54.).

§. 56.

Lehrsatz.

I. *Es giebt für jede Stammzahl* p *immer Werthe von* $z > 0$ *und* $< p$, *aufser* $z = 1$, *von welchen schon niedrigere Potenzen als die* z^{p-1}, *welche nach dem Fermatschen Lehrsatze* (§. 40.) *zu* p *immer den Rest* 1 *läfst, ebenfalls schon diesen Rest geben, so dafs also die Gleichung*

$$1. \quad z^{\varepsilon} = \mathfrak{G}p + 1$$

für diese oder jene z *auch schon für* $\varepsilon < p-1$ *Statt findet.*

II. *Die Werthe von* $\varepsilon < p-1$, *für welche* (1.) *Statt findet, sind alle diejenigen Zahlen* $< p-1$, *welche mit* $p-1$ *einen Theiler* δ *gemein haben, so dafs etwa*

$$2. \quad \varepsilon = \delta\eta \text{ und } p-1 = \delta\tau$$

sein mufs.

III. *Für solche Werthe von* ε *findet die Gleichung* (1.), *wenn* δ *den gröfsten Gemeintheiler von* ε *und* $p-1$ *bezeichnet, für* δ *und für nicht mehr verschiedene Werthe von* z *Statt.*

IV. *Für alle ε, die mit $p-1$ keinen Theiler >1 gemein haben, findet die Gleichung* (1.) *nur für den einzigen Werth* 1 *von* z *Statt.*

V. *Die Werthe von ε, für welche die Gleichung* (2.) *Statt findet, sind aber keineswegs immer die kleinsten, sondern es kann, wenn* (1.) *von irgend einem* z *erfüllt wird, auch für einen noch kleineren Werth von ε schon, für dasselbe* z, $z^{\varepsilon}=\mathfrak{G}p+1$ *sein.*

Beispiele (aus Taf. I.). Zu I. Wie die Tafel zeigt ist z. B. schon $13^3=\mathfrak{G}p+1$, $11^4=\mathfrak{G}p+1$, $9^5=\mathfrak{G}p+1$ u. s. w.

Zu II. Die Zahlen $<p-1$, welche mit $p-1=60$ einen Theiler >1 gemein haben, sind folgende:

$$3.\ \begin{cases} 1,2,3,4,5,6,8,10,12,14,15,16,18,20,21,22,24,25,26,27,28,30,32,33,\\ 34,35,36,38,39,40,42,44,45,46,48,49,50,51,52,54,55,56,57,58.\end{cases}$$

Für alle diese Werthe des Exponenten ε kommt, wie die Tafel zeigt, unter den Werthen von r schon der Rest 1 vor.

Zu III. Der *gröfste* Gemeintheiler von ε und $p-1$ ist z. B. für $\varepsilon=55$, $\delta=5$, und der Tafel zufolge wird die Gleichung (1.) für die $\delta=5$ Werthe 1, 9, 20, 34 und 58 von z erfüllt.

Zu IV. Für $\varepsilon=7$, 11, 13, 49 etc., die mit $p-1$ *keinen* Theiler >1 gemein haben, wird die Gleichung (1.), wie die Tafel zeigt, nur durch den einzigen Werth 1 von z erfüllt.

Zu V. Es ist $9^{45}=\mathfrak{G}p+1$, aber auch schon 9^5, 9^{10}, 9^{15} u. s. w. ist $=\mathfrak{G}p+1$.

Beweis *A*. Man setze

$$4.\quad z^{\gamma}=\mathfrak{G}p+r,$$

wo $r>0$ und $<p$, so ist

$$5.\quad z^{\gamma\delta}=\mathfrak{G}p+r^{\delta}\ (\text{§. 12. 20.}),$$

und da

$$6.\quad z^{\gamma\delta}=z^{p-1}\ (2.)=\mathfrak{G}p+1\ (\text{§. 40.})$$

ist, so ist aus (5. und 6.)

$$\mathfrak{G}p+r^{\delta}=\mathfrak{G}p+1 \text{ oder}$$
$$7.\quad r^{\delta}=\mathfrak{G}p+1,$$

so wie auch

$$8.\quad r^{\delta\eta}=(\mathfrak{G}p+1)^{\eta}=\mathfrak{G}p+1^{\eta}=\mathfrak{G}p+1=r^{\varepsilon}.$$

Nun sind δ und $\varepsilon<p-1$, also giebt es immer Zahlen $r>0$ und $<p-1$, und folglich Werthe von z, von welchen schon *niedrigere* als die $p-1$te Potenz zu p den Rest 1 lassen; gemäfs (I.).

B. Was in (*A.*) bewiesen, gilt für *jeden* Theiler δ von $p-1$, also auch für jedes ε, welches mit $p-1$ irgend einen Theiler $\delta > 1$ gemein hat. Gemäfs (II.).

C. Die Gleichung (7.) findet nach (§. 54. I.) hier für den bestimmten Werth 1 des Restes für δ und für nicht mehr verschiedene Werthe von z (hier r) Statt; also wenn δ der *gröfste* Gemeintheiler von ε und $p-1$ ist, auch für δ verschiedene Werthe, mithin auch die Gleichung (8.) oder (1.) für eben so viele Werthe, und für nicht mehrere. Gemäfs (III.).

D. Hat ε keinen Theiler > 1 mit $p-1$ gemein, so durchläuft nach (§. 55. II.) in

$$9. \quad z^{\varepsilon} = \mathfrak{G}p + r$$

r alle die Zahlen 1, 2, 3, 4, ... $p-1$: also findet die Gleichung (1.) in diesem Fall nur für den einzigen Werth 1 von z Statt; gemäfs (IV.).

E. Nach (II.) giebt es Werthe von $z > 1$, die für jeden *Theiler* δ von $p-1$ die Gleichung

$$10. \quad z^{\delta} = \mathfrak{G}p + 1$$

erfüllen. *Dieselben* Werthe von z erfüllen aber auch die Gleichung

$$11. \quad z^{\delta\eta} = z^{\varepsilon} = \mathfrak{G}p + 1;$$

denn (10.) giebt

$$12. \quad z^{\delta\eta} = (\mathfrak{G}p + 1)^{\eta} = \mathfrak{G}p + 1^{\eta} = \mathfrak{G}p + 1.$$

Also die z, welche die Gleichung (1.) erfüllen, können auch schon der Gleichung (10.) genugthun, in welcher $\delta < \varepsilon$ ist.

Anm. *F.* Die gegenwärtigen Sätze beruhen auf (§. 54. und 55.).

(Die Fortsetzung folgt.)

27.

Erwiderung auf den Artikel 23. im 26sten Bande dieses Journals.

(Von Herrn Prof. *Minding* in Dorpat.)

In diesem Artikel hat Herr Dr. *Magnus* gegen die Regel, welche ich im 22sten Bande d. Journ. zur Bestimmung des Grades einer durch Elimination entstehenden Gleichung aufgestellt habe, eine Einwendung erhoben, welche jedoch durch eine von ihm nur nicht beachtete Stelle des angefochtenen Aufsatzes schon erledigt wird. Nachdem nämlich S. 180 des 22sten Bandes die allgemeine Regel in ihrer Einfachheit, d. h. ohne alle Rücksicht auf specielle Relationen, welche zwischen den Coëfficienten der beiden vorgelegten Gleichungen Statt finden können, aufgestellt ist, heifst es daselbst weiter ausdrücklich so:

„*In besondern Fällen kann man noch die Werthe von* $c_1, c_2, \ldots c_n$ *berücksichtigen, um zu sehen, ob der Coëfficient des höchsten Gliedes in einem der Factoren* $f(x, y_1) \ldots$ *von* ψx*, und mithin in* ψx *selbst, vielleicht gerade Null wird; und in einem solchen Falle wird man genöthigt sein, auch die folgenden Glieder der Reihen für* $y_1, y_2, \ldots y_n$ *theilweise in Rechnung zu bringen;* es wird jedoch nicht erforderlich sein, diese Andeutung hier weiter auszuführen; vielmehr ist klar, dafs *im Allgemeinen* der obige Werth (7.) den wirklichen Grad des Polynoms ψx darstellt."

In diesen wenigen Zeilen, welche die meiner Arbeit widerfahrene Critik übergangen hat, ist das Mittel zur Hebung derjenigen Schwierigkeit, auf welcher der Einwurf des Herrn Dr. *Magnus* beruht, deutlich angegeben. Es kann in besondern Fällen nöthig sein, nicht blofs das erste, sondern auch noch einige folgende Glieder der Reihen für $y_1, y_2, \ldots y_n$ zu berücksichtigen; und zwar ist dies dann nöthig, wenn in irgend einem der Factoren $f(x, y_1), f(x, y_2), \ldots f(x, y_n)$ von ψx der Coëfficient derjenigen Potenz von x, welche sich, ohne noch den Werth von c_1 oder $c_2 \ldots$ oder c_n in Betracht zu ziehen, als die höchste darbietet, durch Einführung dieses Werthes gerade *Null* wird. In dem von Herrn Dr. *Magnus* an-

geführten Beispiele ist die höchste Potenz von x, welche sich sowohl in $f(x, y_1)$ als in $f(x, y_2)$ zunächst darbietet, die dritte; vermöge der besondern Werthe $c_1 = 2$ und $c_2 = 4$ erhält sie aber in beiden Ausdrücken den Coëfficienten Null, wodurch man genöthigt wird, nachfolgende Glieder der Reihen für y_1 und y_2 zu berücksichtigen, und zwar zwei Glieder von y_1: hingegen, weil in $f(x, y_2)$ auch die zweite Potenz von x den Coëfficienten Null bekommt, drei Glieder von y_2. Setzt man nemlich $y_1 = 2x - 2 + \dots$ und $y_2 = 4x - 2 - \frac{1}{2x} + \dots$, so erhält man $f(x, y_1) = -8x^2 + \dots$ und $f(x, y_2) = 6x + \dots$, also $k_1 = 2$ und $k_2 = 1$, folglich ist der Grad der Endgleichung $k_1 + k_2 = 3$; wie erforderlich. Will man aber in solchen Fällen die von mir ausdrücklich für dieselben vorbehaltene Berücksichtigung der folgenden Glieder der Reihen für $y_1, y_2, \dots y_n$ unterlassen, wie es Herr Dr. *Magnus* gethan hat, so kommt man freilich auf Unrichtiges.

Solche besondere Fälle können nicht blofs in numerischen, sondern auch in rein-litteralen Gleichungen vorkommen; wenn nemlich die Coëfficienten der einen Gleichung nicht gänzlich unabhängig von denen der andern sind.

Dorpat, den 24. April 1844.

Fac-simile einer Handschrift von Carnot

Soient M la masse du canon et de son affut.
V leur vitesse après le départ du boulet. m la masse
de ce boulet u sa vitesse au moment de son départ
et enfin K la quantité des forces vives que fait naître
la combustion de la charge donnée de poudre.

La réaction entre le boulet d'une part et le
Canon avec son affut de l'autre, étant égale à l'action
on aura d'abord $MV = mu$ - - (A)

De plus la charge de poudre étant donnée la
force vive exprimée par K est invariable, quel que
soit le recul et cette somme est $MV^2 + mu^2$ on
aura donc aussi $MV^2 + mu^2 = K$ — —(B)

Comparant les deux équations (A) et (B)
pour éliminer V on aura

$$u^2 = K \frac{M}{m \cdot (M+m)}$$

or on suppose que m est une masse très-petite
à l'égard de M parceque le boulet est toujours
très léger en comparaison du canon et de son affut
donc on peut négliger m en comparaison de M
donc l'équation se réduit à $u^2 = K \frac{M}{Mm}$ ou
$u = \sqrt{\frac{K}{m}}$ ce qui fait voir que la vitesse
du boulet est toujours sensiblement indépendante
du poids du canon dès que celui-ci est fort grand
par rapport à l'autre —.



Tafel I.

Sie giebt die Reste* r *an, welche bleiben, wenn man die 1te, 2te, 3te, ... bis* $p-1=60$*te Potenz der Zahlen* $z=1, 2, 3, 4, \dots 60$ $(=p-1)$ *durch die Stammzahl* $p=61$ *dividirt.

In der obersten horizontalen Zeile stehen die Zahlen $z=1, 2, 3, 4, \dots p-1=60$; in der ersten verticalen Reihe links stehen die Exponenten ε der Potenzen dieser Zahlen z, und in den dazu correspondirenden horizontalen Zeilen die Reste r aus

$$z^{\varepsilon} = \mathfrak{G}p+r.$$

Z. B. die Zahlen 1, 54, 41, 49, 46, 18 etc. in der 19ten horizontalen Zeile sind die Reste r der $\varepsilon=19$ten Potenzen von 1, 2, 3, 4, 5, 6 etc. dividirt durch $p=61$.

Nachricht für den Buchbinder. Die Tafel wird von diesem Blatte nicht abgeschnitten, sondern bleibt an demselben fest und wird am Ende des Hefts eingebunden, so dafs die Tafel wie eine Figurentafel ganz aus dem Buche herausgeschlagen werden kann.

1	1	2	3	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
2	1	4	9	57	14	34	56	19	45	12	42	13	47	22	60	39	20	3	49	36	25	16	9	4	1
3	1	8	27	27	11	52	34	24	28	52	41	1	60	41	11	37	3	37	23	28	58	58	34	53	60
4	1	16	20	16	13	58	25	56	12	22	56	47	13	57	1	57	34	9	22	15	15	12	20	16	1
5	1	32	60	14	32	60	13	29	40	14	14	13	14	48	50	40	60	50	29	32	47	13	1	29	60
6	1	3	58	58	60	20	58	27	52	20	34	1	1	34	60	27	9	27	41	52	9	9	58	3	1
7	1	6	52	5	21	27	57	2	31	46	39	47	48	19	11	35	41	28	18	54	16	25	9	55	60
8	1	12	34	12	47	9	15	25	22	57	25	13	47	16	1	16	58	20	57	42	42	22	34	12	1
9	1	24	41	41	50	3	20	38	53	3	52	1	60	52	50	23	27	23	28	53	34	34	20	37	60
10	1	48	1	13	48	1	47	48	14	13	13	47	13	47	60	14	1	60	48	48	13	47	1	48	1
11	1	35	3	19	29	41	22	51	6	36	49	13	14	46	11	43	52	8	30	17	57	56	58	26	60
12	1	9	9	9	1	34	9	58	20	34	58	1	1	58	1	58	20	58	34	20	20	20	9	9	1
13	1	18	27	46	40	52	12	54	26	5	45	46	48	36	50	30	3	24	6	2	22	42	34	43	60
14	1	36	20	25	14	58	16	4	46	42	57	13	47	56	60	5	34	52	19	49	12	15	20	36	1
15	1	11	60	60	11	60	1	50	11	60	60	1	60	60	11	11	60	11	60	11	1	1	1	50	60
16	1	22	58	22	13	20	42	15	57	16	15	47	13	12	1	12	9	34	16	56	56	57	58	22	1
17	1	44	52	4	32	27	56	35	7	59	19	13	14	39	50	2	41	33	9	30	25	16	9	17	60
18	1	27	34	34	60	9	34	41	3	9	20	1	1	20	60	41	58	41	52	3	58	58	34	27	1
19	1	54	41	45	21	3	25	55	10	39	5	47	48	4	11	17	27	38	2	43	15	12	20	7	60
20	1	47	1	47	47	1	13	47	13	47	47	13	47	13	1	13	1	1	47	47	47	13	1	47	1
21	1	33	3	3	50	41	58	8	23	41	27	1	60	27	50	53	52	53	37	23	9	9	58	28	60
22	1	5	9	56	48	34	57	39	36	15	22	47	13	42	60	19	20	3	46	45	16	25	9	5	1
23	1	10	27	49	29	52	15	30	59	4	36	13	14	45	11	54	3	37	44	35	42	22	34	50	60
24	1	20	20	20	1	58	20	9	34	58	9	1	1	9	1	9	34	9	58	34	34	34	20	20	1
25	1	40	60	48	40	60	47	21	32	48	48	47	48	14	50	32	60	50	11	40	13	47	1	21	60
26	1	19	58	42	14	20	22	49	5	25	12	13	47	15	60	46	9	27	36	4	57	56	58	19	1
27	1	38	52	52	11	27	9	33	37	27	3	1	60	3	11	28	41	28	53	37	20	20	9	23	60
28	1	15	34	15	13	9	12	16	42	56	16	47	13	25	1	25	58	20	56	22	22	42	34	15	1
29	1	30	41	36	32	3	16	17	18	19	4	13	14	5	40	55	27	23	35	51	12	15	20	31	60
30	1	60	1	1	60	1	1	60	60	1	1	1	1	1	60	60	1	60	60	60	1	1	1	60	1
31	1	59	3	39	21	41	42	18	17	45	46	47	48	49	11	10	52	8	7	6	56	57	58	2	60
32	1	57	9	57	47	34	56	42	16	2	42	13	47	22	1	22	20	58	12	25	25	16	9	57	1
33	1	53	27	27	50	52	34	37	33	52	41	1	60	41	50	24	3	24	38	33	58	58	34	8	60
34	1	45	20	16	48	58	25	5	49	22	56	47	13	57	60	4	34	52	39	46	15	12	20	45	1
35	1	29	60	14	29	60	13	32	21	14	14	13	14	48	11	21	60	11	32	29	47	13	1	32	60
36	1	58	58	58	1	20	58	34	9	20	34	1	1	34	1	34	9	34	20	9	9	9	58	58	1
37	1	55	52	5	40	27	57	59	30	46	39	47	48	19	50	26	41	33	43	7	16	25	9	6	60
38	1	49	34	12	14	9	15	36	39	57	25	13	47	16	60	45	58	41	4	19	42	22	34	49	1
39	1	37	41	41	11	3	20	23	8	3	52	1	60	52	11	38	27	38	33	8	34	34	20	24	60
40	1	13	1	13	13	1	47	13	47	13	13	47	13	47	1	47	1	1	13	13	13	47	1	13	1
41	1	26	3	19	32	41	22	10	55	36	49	13	14	46	50	18	52	53	31	44	57	56	58	35	60
42	1	52	9	9	60	34	9	3	41	34	58	1	1	58	60	3	20	3	27	41	20	20	9	52	1
43	1	43	27	46	21	52	12	7	35	5	45	47	48	36	11	31	3	37	55	59	22	42	34	18	60
44	1	25	20	25	47	58	16	57	15	42	57	13	47	56	1	56	34	9	42	12	12	15	20	25	1
45	1	50	60	60	50	60	1	11	50	60	60	1	60	60	50	50	60	50	11	50	1	1	1	11	60
46	1	39	58	22	48	20	42	46	4	16	15	47	13	12	60	49	9	27	45	5	56	57	58	39	1
47	1	17	52	4	29	27	56	26	54	59	19	13	14	39	11	59	41	28	51	31	25	16	9	44	60
48	1	34	34	34	1	9	34	20	58	9	20	1	1	20	1	20	58	20	9	58	58	58	34	34	1
49	1	7	41	45	40	3	25	6	51	39	5	47	48	4	50	44	27	23	59	18	15	12	20	54	60
50	1	14	1	47	14	1	13	14	48	47	47	13	47	13	60	48	1	60	14	14	47	13	1	14	1
51	1	28	3	3	11	41	58	53	38	41	27	1	60	27	11	8	52	8	24	38	9	9	58	33	60
52	1	56	9	56	13	34	57	22	25	15	22	47	13	42	1	42	20	58	15	16	16	25	9	56	1
53	1	51	27	49	32	52	15	31	2	4	36	13	14	45	50	7	3	24	17	26	42	22	34	10	60
54	1	41	20	20	60	58	20	52	27	58	9	1	1	9	60	52	34	52	3	27	34	34	20	41	1
55	1	21	60	48	21	60	47	40	29	48	48	47	48	14	11	29	60	11	40	21	13	47	1	40	60
56	1	42	58	42	47	20	22	12	56	25	12	13	47	15	1	15	9	34	25	57	57	56	58	42	1
57	1	23	52	52	50	27	9	28	24	27	3	1	60	3	50	33	41	33	8	24	20	20	9	38	60
58	1	46	34	15	48	9	12	45	19	56	16	47	13	25	60	36	58	41	5	39	22	42	34	46	1
59	1	31	41	36	29	3	16	44	43	19	4	13	14	5	11	6	27	38	26	10	12	15	20	30	60
60	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

